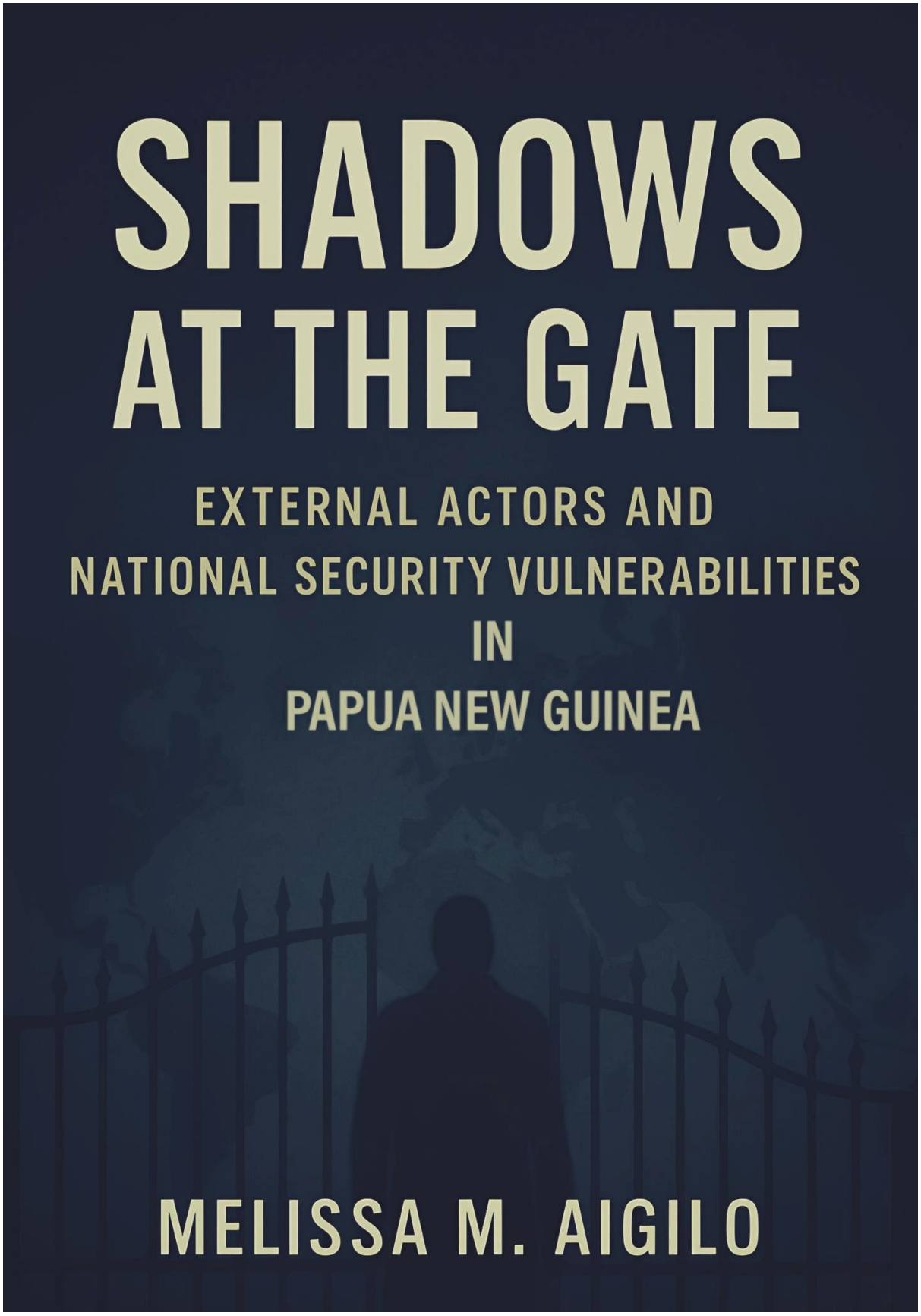
SHADOWS AT THE GATE

EXTERNAL ACTORS AND NATIONAL SECURITY VULNERABILITIES IN PAPUA NEW GUINEA



MELISSA M. AIGILO

SHADOWS AT THE GATE: EXTERNAL ACTORS AND NATIONAL SECURITY VULLNERABILITIES

MELISSA M. AIGILO

Shadows at the Gate: External Actors and National Security Vulnerabilities by Melissa M. Aigilo

© 2025 Melissa M. Aigilo
All rights reserved.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without prior written permission from the author, except for brief quotations used in reviews or academic analysis.

This book is a work of non-fiction. The author has made every effort to ensure the accuracy and reliability of the information contained herein. However, the author and publisher disclaim any liability for errors, omissions, or consequences arising from the use of this book.
Published in Port Moresby, Papua New Guinea
First Edition — 2025

DISCLAIMER

Shadows at the Gate: External Actors and National Security Vulnerabilities in Papua New Guinea is written from a civilian perspective and reflects the author's personal research and analysis.

All information presented in this work has been collected from publicly available materials. The author does not claim to represent or speak on behalf of any government, law enforcement, or intelligence agency.

While every effort has been made to ensure accuracy, the information may not be complete or up to date. Readers are responsible for independently verifying any facts, statistics, or claims through the appropriate state or official agencies. The author, publisher, and distributors of this book assume no responsibility or liability for any consequences arising from the use of this information.

Dedication

“For the men and women who walk the frontline of security, who guard our borders so that we may sleep well at night. We rest because you stand watch.”

Acknowledgements

I give thanks to God, whose watchful eyes are ever vigilant, silently observing with the precision of an intelligence officer—guiding, protecting, and unseen.

I acknowledge as always, my instructor in intelligence and tradecraft, Chief Sergeant Detective Christopher Mursau, RPNGC (ret.), whose guidance, discipline, and insights shaped my understanding of the unseen and the strategic mind required to navigate it.

Table of Contents

Disclaimer
Dedication
Acknowledgements

Chapter 1: The Anatomy of Threats ----------1

- Defining External Actors: State vs Non-State
- Intelligence Threat Spectrum: Cyber, Physical, Financial
- Historical Threats to PNG's Sovereignty
- Early Warning Indicators and Threat Signatures

Chapter 2: Mapping the Shadows----------20

- Geopolitical Hotspots Affecting PNG
- Networks and Cells: Identifying External Influence
- Financial and Resource Channels of Threat Actors
- Shadow Zones: Areas Vulnerable to Undetected Operations

Chapter 3: Vulnerabilities Within ----------26

- Critical Infrastructure Weak Points (Ports, Energy, Communications)
- Insider Threats: Corruption, Compromise, Human Factor
- Technology and Cybersecurity Gaps
- Lessons from Previous Security Breaches

Chapter 4: Intelligence Collection and Analysis----------43

- Open-Source Intelligence (OSINT) in PNG Context
- Human Intelligence (HUMINT): Handling Sources Safely
- Signals Intelligence (SIGINT) and Emerging Technologies
- Analysis Tools: Threat Assessment Models and Probabilities

Chapter 5: External Actors' Methods and Tactics----------48

- Cyber Operations and Digital Espionage
- Influence Operations and Social Manipulation
- Covert Funding and Smuggling Networks
- Case Studies: Lessons from Asia-Pacific Threat Actors

Chapter 6: National Security Policy and Preparedness--------56

- PNG's Security Framework: Legal and Operational Overview
- Coordination Between Agencies and Military Intelligence
- Crisis Response and Contingency Planning
- Exercises and Scenario-Based Threat Simulations

Chapter 7: Countermeasures and Strategic Defense-------64

- Mitigation Strategies for Identified Vulnerabilities
- Counterintelligence Measures: Detection and Disruption
- Technology-Enhanced Defense Systems
- Building Resilience: Training, Awareness, and Community Engagement

Chapter 8: Threat Assessment in Action--------70

- Real-Time Threat Monitoring and Intelligence Cycle
- Profiling High-Risk Entities
- Decision-Making Under Uncertainty
- Case Studies: Prevented Attacks and Lessons Learned

Chapter 9: Cyber Frontiers and Emerging Threats-------75

- Digital Espionage Tactics
- AI and Automation in Threat Detection
- Social Media and Psychological Operations
- Preparing for Future Technological Vulnerabilities

Chapter 10: Insider Threats and Human Factor-------81

- Detecting Compromised Personnel
- Behavioral Analysis and Warning Signs
- Loyalty, Coercion, and Blackmail Scenarios
- Strengthening Internal Security Culture

Chapter 11: International Cooperation and Intelligence Sharing-----86

- Regional Partnerships: PNG and Pacific Allies
- Legal Frameworks for Cross-Border Intelligence
- Case Studies: Collaborative Operations
- Risks of Miscommunication and Leakage

Chapter 12: The Path Forward – Resilience and National Security---------90

- Long-Term Strategy for Threat Prevention
- Strengthening Institutions and Intelligence Capacity
- Community Engagement in National Security

Lessons Learned and Preparing PNG for the Future

Forward

Preface

Reference --------105

Foreword

In an era where small states navigate a complex interplay of geopolitics, transnational crime, and emerging technologies, Papua New Guinea occupies a uniquely vulnerable yet strategic position in the Pacific. *Shadows at the Gate* seeks to illuminate the subtle, often invisible forces that challenge our nation's sovereignty and stability.

This book is not merely an academic exercise; it is an operational-level analysis rooted in real-world intelligence principles. Drawing on both historical precedents and contemporary developments, it examines how external actors—state and non-state alike—leverage economic, political, military, and criminal pathways to exert influence over national systems. Through methodical research and structured insight, the work highlights the vulnerabilities inherent in our critical infrastructure, governance frameworks, and security institutions.

The chapters within provide a roadmap for understanding the anatomy of threats, the intelligence processes required to anticipate them, and the frameworks necessary for strategic mitigation. It bridges theory and practice, offering both security practitioners and policymakers a lens through which to evaluate risk, prioritize responses, and safeguard PNG's national interest.

While this book addresses national security at a systemic level, it also underscores the human dimension of intelligence work—the vigilance, analysis, and ethical responsibility required to operate effectively in a landscape where the line between opportunity and threat is often blurred.

Shadows at the Gate is written with the conviction that informed awareness is the first step toward resilience. For those tasked with protecting our nation, understanding the forces at play is not optional—it is imperative.

PREFACE

Papua New Guinea sits at a crossroads of cultures, trade, and strategic interest. Its mountains, rivers, and remote coastlines are not just landscapes—they are corridors and cover for actors whose intentions are often hidden from view. In the quiet corners of Port Moresby, Lae, and even the smallest highland villages, foreign agents operate with subtlety, testing the resilience of our communities, institutions, and intelligence networks.

This book is written from the perspective of someone who has observed these forces firsthand. It traces the methods and networks of external actors—state and non-state alike—who seek to influence politics, exploit resources, and manipulate information. From covert funding and surveillance to cyber operations and human intelligence recruitment, their presence is real, persistent, and often invisible to the public eye.

Through these pages, readers will gain insight into how espionage manifests in Papua New Guinea, how vulnerabilities arise and how they can be mitigated. More than analysis, it is a call for awareness, vigilance, and understanding of the threats that operate in our shadows. For the safety and sovereignty of our nation, knowing the enemy is not optional—it is essential.

Melissa Majella Aigilo
December 10, 2025

Chapter 1: The Anatomy of Threats

Defining External Actors: State vs Non-State

External actors are entities that operate beyond the formal boundaries of a nation-state yet exert significant influence over its political stability, economic security, and internal order. In contemporary security studies, external actors are recognized as central drivers of conflict, coercion, cooperation, and destabilization in both developed and fragile states (Buzan & Hansen, 2009; Waltz, 1979). Their influence may be overt through diplomacy and aid, or covert through espionage, proxy violence, and economic manipulation.

External actors are broadly categorized into state actors and non-state actors.

State Actors

State actors are formal representatives of sovereign governments that operate with legal authority, institutional backing, and strategic national intent. These include foreign governments, intelligence agencies, militaries, diplomatic missions, and state-owned enterprises acting in strategic sectors (Waltz, 1979; Nye, 2004).

State power is exercised through diplomacy, Military force, economic leverage and intelligence operations. Modern state influence increasingly includes cyber operations, information warfare, and political interference beyond territorial borders (Rid, 2020; Betts, 2007).

State actors pursue long-term strategic objectives such as:

- Resource access
- Political alignment
- Military positioning
- Economic dependency
- Regional dominance

Although state interactions often appear cooperative under the cover of diplomacy, trade, or development assistance, security scholars caution that these engagements frequently conceal competitive geopolitical motivations (Mearsheimer, 2014; Buzan et al., 1998).

Non-State Actors

Non-state actors are entities which operate independently of formal government authority, yet exert substantial security impact within and across national borders. These include transnational criminal organizations, terrorist groups, insurgents, private Military contractors, cybercrime syndicates, and illicit trafficking networks (Williams, 2008; Shelley, 2014).

Non-state actors exploit:

- Weak governance
- Porous borders
- Corruption
- Informal economies
- Digital platforms

Their operations typically involve human trafficking, arms smuggling, illicit resource extraction, financial crime, cyber intrusion, targeted violence, and mass disinformation (UNODC, 2023; Shelley, 2014).

Unlike state actors, non-state actors are driven primarily by profit, ideology, or coercive power rather than diplomatic legitimacy. They adapt rapidly to enforcement pressure and shift alliances with minimal political constraint (Kaldor, 2012).

The Convergence of State and Non-State Actors

One of the most threatening developments in modern security is the convergence between state and non-state actors. This hybrid threat environment surfaces when states use criminal groups, militant factions, or corporate fronts as proxies to push forward their strategic interests while maintaining plausible deniability. (Hoffman, 2007; Rid, 2020).

Examples of convergence include:

- State-sponsored organized crime
- Militant groups funded by foreign intelligence services
- Corporations used as espionage platforms
- Armed groups shielded by political patrons

This fusion blurs the boundary between war, crime, and diplomacy, making attribution, deterrence, and legal accountability extremely difficult for national security institutions (Betts, 2007; Hoffman, 2007).

Why the Distinction Matters for National Security

Distinguishing between state and non-state external actors is important for:

- Intelligence collection and threat attribution
- Counterintelligence operations
- Border and maritime security planning
- Economic and infrastructure protection
- Strategic defense policymaking

Failure to correctly identify the nature of an external actor results in flawed intelligence assessments, ineffective countermeasures, and delayed national responses—often with irreversible strategic consequences (Lowenthal, 2020; Betts, 2007).

Intelligence Threat Spectrum: Cyber, Physical, Financial

These threats emerge across a complex and interconnected intelligence threat spectrum that spans cyber, physical, and financial domains. Contemporary security scholars widely agree that these three domains now operate as an integrated system of attack rather than as isolated threat categories (Rid, 2020; Betts, 2007; Kaldor, 2012). For vulnerable or developing states such as Papua New Guinea (PNG), this convergence presents an elevated national security risk due to limited surveillance

capacity, regulatory weaknesses, and high exposure to transnational influence (PNG National Security Policy, 2013).

Cyber Threats

Cyber threats can be described as hostile activities conducted through digital networks to compromise national security, economic stability, critical infrastructure, and public trust. These include cyber espionage, data theft, system sabotage, online disinformation, election interference, and financial system intrusion (Rid, 2020; Nye, 2010).

Cyber operations are especially attractive to both state and non-state actors because they are:

- Low cost
- High impact
- Difficult to attribute
- Easily deniable

Rid (2020) recognizes cyber operations as a core instrument of modern political warfare, where espionage, sabotage, and psychological influence operate simultaneously within civilian digital systems. From an intelligence perspective, cyber space has become a primary battlefield for pre-conflict shaping operations—way before physical violence occurs.

In the Pacific context, PNG's exposure to cyber threats has risen sharply with the expansion of mobile banking, digital government services, and online communication platforms. The PNG National Cyber Security Strategy recognizes that hostile cyber activity now presents a direct threat to national sovereignty, public confidence, and economic integrity (Government of Papua New Guinea, 2021).

Cyber threats directly enable both physical attacks (through surveillance, tracking, and targeting) and financial crimes (through digital fraud and system compromise), making them the primary entry point of modern hybrid warfare.

(National Security & Intelligence Context – PNG Adapted)

Threat Category	Threat Actor	Primary Target	Method of Attack	Strategic Objective	National Security Impact	PNG Relevance Level
Espionage	Foreign State Actors	Defence networks, Intelligence databases	Phishing, Zero-day exploits, Malware implants	Steal classified information	Compromises sovereignty and operational security	Critical
Cyber Sabotage	State & Proxy Actors	Power grids, telecoms, ports, aviation	SCADA intrusion, ransomware	Disrupt national operations	Infrastructure paralysis	High
Influence Operations	Foreign Intelligence Units	Public opinion, elections, social stability	Disinformation, bot campaigns	Shape political outcomes	Undermines democratic stability	High
Cyber Terrorism	Ideological Extremists	Government websites, emergency services	Website defacement, data destruction	Spread fear and instability	Public panic, confidence erosion	Moderate
Cybercrime (Organized)	Transnational Crime Syndicates	Banks, mobile money, citizens	Phishing, SIM-swap, hacking	Financial theft	Economic destabilization	Critical
Insider Cyber Threat	Disgruntled staff	Defence, Police, Govt agencies	Data leaks, unauthorized access	Personal gain or retaliation	Severe intelligence compromise	Critical
Supply Chain Attacks	Foreign Tech Providers	Government systems	Backdoors, firmware compromise	Long-term access	Invisible persistent threat	High
Surveillance & Tracking	Foreign Intelligence	Key officials, officers	Spyware, phone hacking	Monitor movements & decisions	Strategic manipulation	High

Psychological Cyber Ops	Foreign & Domestic Actors	Military morale, public trust	Deepfakes, fake leaks	Confuse, divide, discredit	Morale breakdown	High
Data Harvesting	Tech Corporations / Data Brokers	Citizens & agencies	App permissions, metadata scraping	Build intelligence datasets	Loss of digital sovereignty	Moderate

Diagram 1: Cyber Threat Matrix

CYBER DOMAIN LEVELS OF WARFARE

1. Tactical Level – Individual hacking, phishing, SIM-swap crimes
2. Operational Level – Coordinated attacks on banks, telecoms, ports
3. Strategic Level – Espionage against Defence, Intelligence & Cabinet systems

PNG is currently most vulnerable at Tactical and Operational levels, with rising exposure at Strategic level due to:

- Digital banking expansion
- Mobile-based government services
- Foreign telecommunications infrastructure
- Limited cyber defence personnel

CYBER THREAT DYNAMICS UNIQUE TO PNG

- High mobile phone penetration with low cyber awareness
- Weak endpoint security in provincial government networks
- Heavy reliance on foreign ICT infrastructure
- Limited cyber intelligence overlap between:

  - PNGDF
  - RPNGC
  - NICTA
  - National Cyber Security Centre

This creates intelligence blind spots exploitable by:

- Transnational syndicates
- Foreign intelligence services
- Political influence operators

INTELLIGENCE WARNING INDICATORS

Early signs of escalation include:

- Sudden phishing spikes targeting uniformed services
- Fake social media accounts targeting officers
- SIM-swap incidents involving senior officials
- Encrypted messaging infiltration
- Leaked documents appearing online

These are pre-attack shaping indicators, not isolated crimes.

STRATEGIC ASSESSMENT (INTEL DOCTRINE)

Cyber threats to PNG are no longer technical risks — they are now:

- Sovereignty risks
- Command-and-control risks
- National morale risks
- Economic warfare tools

Cyber is now a primary battlespace, not a support domain.

Physical Threats

Physical threats remain the most visible and kinetic dimension of the intelligence threat spectrum. These include armed attacks, assassinations, sabotage of infrastructure, insurgency, terrorism, border incursions, and violent criminal operations (Hoffman, 2007; Kaldor, 2012).

Kaldor (2012) describes modern conflict as a fusion of state warfare, organized crime, and political violence—what she defines as "new wars." These conflicts are characterized by:

- Irregular forces
- Civilian targeting
- Criminal funding streams
- Weak distinction between combatant and non-combatant

In PNG, physical threats to national security are closely linked to:

- Tribal and communal violence
- Transnational trafficking routes
- Illegal resource extraction
- Border security vulnerabilities
- Firearms proliferation

The PNG Defence White Paper and National Security Policy (2013) both identify internal instability, border control weaknesses, and organized criminal violence as primary physical threat drivers. Physical threats are rarely spontaneous; they are usually enabled by cyber surveillance and financed through illicit financial networks, demonstrating the interdependence of the threat spectrum.

INTELLIGENCE WARNING INDICATORS
(PHYSICAL / KINETIC THREATS)
PRE-INCIDENT RECONNAISSANCE INDICATORS

(Most critical early stage warnings — often missed)

- Repeated sighting of unfamiliar individuals near sensitive facilities
- Mobile phones used to photograph gates, guards, patrols, vehicles
- Vehicles parking repeatedly without clear purpose
- Individuals asking indirect questions about routines or shifts
- Local civilians suddenly showing over-interest in security layouts
- Increased presence of non-local accents or unfamiliar faces
- Sudden drone sightings near compounds or ports

Intel meaning: Target selection and pattern-of-life mapping is underway.

PRE-POSITIONING & LOGISTICS INDICATORS

(Attack capability being assembled)

- Unexplained movement of fuel, chemicals, or large tools
- Stolen vehicles reported near key routes
- Rental properties taken near:
    - Barracks
    - Ports
    - Airports
    - Political offices
- Storage of:
    - Machetes
    - Firearms
    - IED components
- Cash movements inconsistent with normal income
- Sudden recruitment of idle youth or ex-security guards

Intel meaning: Operational capability is being built.

PERSONNEL & INSIDER WARNING INDICATORS

(Most dangerous category)

- Security staff:
    - Requesting schedule changes without clear reason
    - Asking about armoury access or response times
    - Showing sudden hostility, stress or secrecy
- Officers suddenly:
    - Carrying multiple phones
    - Avoiding normal peer contact
    - Showing financial stress with sudden relief
- Unauthorized access attempts to:
    - Vehicle logs

    - Guard rosters
    - CCTV systems

Intel meaning: Insider compromise is forming.

MOBILIZATION & FINAL STAGE INDICATORS

(Attack likely within 24–72 hours)

- Sudden disappearance of known agitators
- Increased encrypted communication traffic
- Sudden travel of suspects toward the target area
- Vehicles staged facing exit routes
- Cash withdrawals in small bundles
- Weapons moved from storage to vehicles
- Last-minute religious or farewell behavior
- At-risk individuals being quietly removed from the area

Intel meaning: Attack window is opening.

CROWD & PUBLIC SPACE INDICATORS

(Urban & event-based threats)

- Groups forming with:
    - Coordinated clothing or symbols
    - Unusual silence or discipline
- Elevated agitation in youth clusters
- Sudden alcohol or drug distribution before gatherings
- Blocking of escape routes (parked vehicles, debris)
- Scouts positioned at high vantage points

Intel meaning: Riot, ambush, or targeted violence is being shaped.

SYMBOLIC & PSYCHOLOGICAL INDICATORS

(Threat signaling phase)

- Graffiti with political or militant messaging
- Threat messages on:
    - Facebook
    - TikTok
    - WhatsApp groups

- Circulation of:
    - Deepfake threats
    - Edited images of targets
- Rumours of:
    - “Something big coming”
    - “Time to send a message”

Intel meaning: Psychological preparation and fear seeding.

STRATEGIC INTELLIGENCE ASSESSMENT

Physical threats in PNG are most likely to emerge from:

- Political instability cycles
- Resource conflict zones
- Transnational crime logistics
- Insider compromise
- Youth gang mobilization
- Foreign proxy agitation

The greatest danger is hybrid threat fusion:

Physical attack supported by cyber surveillance, disinformation, and insider leakage.

Operational Objective	**Strategic Impact**	**PNG Risk Level**	**Phase**		**Threat Activity**	**Probability**
Armed Assault	Gangs, insurgents, criminal groups	Barracks, police posts, convoys	Phase 1	Surveillance	Low but rising	High
Targeted Assassination	Contract killers, political proxies	Officers, leaders, witnesses	Phase 2	Logistics	Moderate	High
IED / Explosive Attack	Insurgents, criminal cells	Roads, gates, events	Phase 3	Insider Shifts	High	Moderate–High

Riot / Urban Unrest	Youth mobs, political agitators	Markets, govt offices	Phase 4	Mobilization	Very High	High
Hostage Taking	Criminal gangs	Expats, officials, pilots	Phase 5	Execution	Imminent	Moderate
Barracks Infiltration	Insider-supported actors	Armouries, dorms	Disguises, stolen badges	Steal weapons, sabotage	Direct defence compromise	Critical
Sabotage (Infrastructure)	Criminal syndicates, proxies	Power, fuel, bridges, telecoms	Arson, mechanical damage	Disrupt economy & response	Operational paralysis	High
Close Protection Breach	Lone attackers, extremists	VIP movements	Stabbing, vehicle ramming	Symbolic murder	National panic	High
Militia Formation	Clan-based groups	Highlands, disputed land	Firearms stockpiling	Territorial control	Internal sovereignty threat	High
Cross-Border Armed Movement	Foreign non-state actors	Border regions	Small arms, foot patrols	Smuggling, influence	Border security erosion	Moderate
Port & Maritime Attack	Criminal syndicates	Ports, ships, LNG	Armed boarding, sabotage	Disrupt trade, smuggle	Economic warfare effect	High
Arson & Destruction	Political mobs, criminals	Courts, schools, stations	Fire setting	Intimidation, chaos	Rule-of-law erosion	High

Diagram 2:Physical / Kinetic Threat Matric

LEVELS OF PHYSICAL THREAT WARFARE

1. Low-Level Violence – Assaults, intimidation, opportunistic crime
2. Organized Criminal Violence – Armed gangs, extortion networks
3. Militant-Style Operations – Ambushes, IEDs, hostage situations

4. Internal Conflict – Clan warfare, militia zones
5. Hybrid Conflict – Physical violence enabled by cyber & information operations

PNG currently operates mostly between Levels 2–4, with Level 5 hybrid threats emerging.

KEY PHYSICAL THREAT MULTIPLIERS IN PNG

- High youth unemployment
- Easy local firearm access
- Political grievance cycles
- Weak early-warning systems
- Insider compromise risk
- Remote terrain & slow response times

These multipliers accelerate threat evolution from low-level crime to organized violence very quickly.

STRATEGIC INTELLIGENCE ASSESSMENT (PHYSICAL DOMAIN)

Physical threats in PNG are not random — they follow:

- Political pressure cycles
- Resource conflict timelines
- Criminal financing routes
- Insider-enabled access
- Perception of weak response

The most dangerous threat form moving forward is:

Hybrid Physical–Cyber–Insider Attacks against security institutions.

Financial Threats

Financial threats involve the manipulation, theft, laundering, or strategic control of money and economic systems to fund destabilization, corruption, crime, or covert influence operations. These

include money laundering, terrorist financing, illegal mining profits, foreign corporate influence, tax evasion, bribery, and economic coercion (Shelley, 2014; UNODC, 2023).

Shelley (2014) highlights that modern security threats are sustained not by ideology alone but by financial ecosystems of crime, where terrorism, corruption, cybercrime, and resource exploitation operate within the same transactional networks.

In PNG, financial threats are directly linked to:

- Illegal logging and fishing
- Unregulated mining operations
- Transnational corruption networks
- Political bribery
- Foreign corporate manipulation

The Financial Analysis and Supervision Unit (FASU) of PNG has repeatedly warned that money laundering and foreign-linked financial crime pose systemic threats to national governance and security stability (FASU PNG, 2020). When financial systems are compromised, they weaken:

- Intelligence operations
- Law enforcement
- Judicial authority
- Political legitimacy

Financial power enables external actors to exert silent control over national decision-making structures without deploying armed force.

Threat Category	Description	Indicators / Signatures	Likelihood	Impact	Overall Risk
1. Illicit Financial Flows (IFFs)	Funds moved illegally into or out of PNG to evade tax, sanctions, or oversight.	Sudden unexplained transfers; shell companies; use of offshore accounts; mismatched trade invoices.	High	High	**Severe**
2. Foreign State Influence via Investment	Strategic foreign states using loans, grants, or	Long-term repayment dependency;	Medium-High	High	**High**

	infrastructure investments to gain political leverage.	opaque loan terms; foreign advisors embedded in ministries; infrastructure tied to foreign control.			
3. Money Laundering (Domestic & Transnational)	Criminal networks using PNG banks, casinos, real estate, or gold trade to clean dirty money.	Cash-heavy businesses; high-value property purchases; politically exposed individuals (PEIs) with inconsistent income.	High	Medium-High	**High**
4. Corruption & Misappropriation of Public Funds	Diversion of government budgets, grants, or land funds for personal or political gain.	Inflated contracts; same contractors winning tenders; incomplete projects; rapid wealth of officials.	High	High	**Severe**
5. Cyber-Financial Crimes	Attacks targeting PNG banks, mobile money systems, government payment systems.	System outages; phishing campaigns; cross-border syndicates targeting BSP/Kina systems; ransomware demands.	Medium	High	**High**
6. Corporate Exploitation in Resource Sector	Companies underreporting extraction volumes, tax evasion, and profit shifting.	Discrepancies between export volumes and declared revenue; use of foreign contractors; unexplained royalty shortfalls.	Medium	High	**High**
7. Community-Level Financial Manipulation	External actors exploiting rural communities through micro-loans, informal credit, land buying.	Predatory loan schemes; foreign buyers approaching rural clans; increase in land disputes.	Medium	Medium	**Moderate**
8. NGO or Aid Funding Diversion	Misuse of donor funds for political or foreign influence.	NGOs with unclear leadership; overseas cash flow; training	Low-Medium	Medium	**Moderate**

		programs with political undertones.			
9. Cryptocurrency & Unregulated Digital Assets	Anonymous funds movement used by organised crime or foreign networks.	Rapid crypto adoption; scams; international wallet addresses interacting with PNG users.	Medium	Medium	**Moderate**
10. Sanctions Evasion Networks	PNG used as a transit point or shell destination for sanctioned states or entities.	Registration of foreign-owned front companies; unusual shipping movements; transactions with sanctioned jurisdictions.	Low	High	**Moderate**

Diagram 3: Financial Threat Matrix

Key Insights

1. PNG is highly vulnerable to IFFs and corruption, which external actors can easily exploit.

2. Financial penetration is often the *first sign* of deeper geopolitical influence.

3. Provincial governments are particularly exposed due to weak oversight.

4. The resource sector remains the largest avenue for covert financial exploitation.

The Integrated Threat Environment

The modern intelligence environment no longer treats cyber, physical, and financial threats as separate categories. Instead, they function as a unified hybrid threat system (Hoffman, 2007; Rid, 2020). A cyber intrusion enables a physical attack; a physical operation is financed through illicit money; financial laundering is protected through cyber anonymization.
This integrated model is now the preferred method of operation for:

- Foreign intelligence services
- Transnational criminal syndicates
- Terrorist financiers
- Illicit corporate networks

For PNG, the convergence of these three threat domains represents a tier-one national security vulnerability, requiring intelligence integration across Military, police, financial regulators, immigration, and cyber agencies (PNG National Security Policy, 2013; Government of PNG, 2021).

Strategic Intelligence Implications

Understanding the cyber–physical–financial threat spectrum is essential for:

- Threat attribution
- Counterintelligence operations
- National risk forecasting
- Critical infrastructure protection
- Election and political system security

Betts (2007) emphasizes that intelligence failure most often occurs not from lack of data, but from the failure to connect financial, cyber, and physical indicators into a single threat picture. In fragile security environments, this failure allows hostile external actors to operate undetected until strategic damage is already irreversible.

Historical Threats to PNG's Sovereignty

Papua New Guinea's (PNG) modern sovereignty has been shaped by a sequence of external and internal threats that range from colonial domination and wartime occupation to internal secessionism, resource-driven contestation, and contemporary geopolitical influence. Understanding these threats requires attention to five overlapping categories: colonial legacy and external administration; wartime invasion and strategic vulnerability; internal secession and civil conflict; economic/extractive pressures and private Military involvement; and contemporary geostrategic competition.

Colonial administration and the legacy of external authority

PNG's modern borders and administrative structures were consolidated under successive external administrations—first German and British in the north, and later Australian administration of Papua and New Guinea—which left institutional patterns, land-tenure tensions and dependence on external

security arrangements that continue to affect sovereignty perceptions. Australia's administration (officially from the early 20th century until independence in 1975) created centralized bureaucratic linkages and security relationships that have shaped PNG's post-colonial decision-making and defence posture. These legacies mean sovereignty has often been negotiated in practice through arrangements with external partners.

Wartime occupation and strategic vulnerability

During the Pacific War (1942–45) PNG was a major theatre of conflict, suffering Japanese incursions and Allied counter-operations. The intensity of these campaigns exposed the territory's strategic vulnerability and demonstrated how external great-power conflict could directly determine control over PNG territory and resources. Wartime legacies reinforced the need for external security cooperation in the post-war era and shaped PNG's later security calculus.

Internal secessionism: the Bougainville conflict and governance fractures

Perhaps the most significant internal threat to PNG's sovereignty in the post-independence era was the Bougainville conflict (late 1980s–1990s). Sparked by grievances over the Panguna mine, uneven economic benefits, and ethno-political tensions, the insurgency escalated into widespread violence that threatened the state's territorial control and legitimacy. The central government's responses—including militarized operations and the controversial engagement of external mercenary forces during the Sandline episode—exposed limits in state capacity and raised questions about how sovereignty should be defended or exercised internally. The peace process that followed, and the later autonomy and referendum arrangements, underscore how internal fragmentation can materially alter state sovereignty.

Resource extraction, land disputes and non-state actors.

Resource extraction (mining, logging, and large-scale agriculture) has repeatedly placed sovereignty under strain. Concessions to multinational companies, contested customary land rights, and the social dislocations around large projects create governance vacuums that external actors can exploit—undermining local authority and provoking conflict. The Panguna experience demonstrates how resource grievances translate into political mobilization that challenges central control. More recently,

discussions about private Military companies, security contractors, and the limits of state monopoly on force highlight how non-state actors can erode sovereign control when the state lacks capacity or legitimacy.

Geostrategic influence and modern state-level pressures.

In the contemporary era, PNG's sovereignty is also tested by geopolitical manoeuvring in the Pacific. Economic diplomacy, infrastructure financing (including Chinese Belt and Road engagements), and security partnerships (notably with Australia and other partners) all produce choices that can expand state capacity but may also create dependency or political friction. Recent regional developments—greater great-power interest in the Pacific and new bilateral security frameworks—illustrate that sovereignty is not only an internal property but also a negotiated position in an external strategic environment. These dynamics require PNG to balance foreign partnerships that provide security and development with the imperative to retain autonomous policy space.

Synthesis: threat vectors and resilience

Historically, PNG's main sovereignty threats flowed from (1) external occupation or administrative domination, (2) internal fracture and secession, (3) resource-driven local conflicts and non-state armed actors, and (4) contemporary geostrategic competition that can reshape state decision-space. The country's resilience has depended on negotiated settlements (e.g., Bougainville peace processes), institutional capacity building, and the careful management of external ties. For contemporary policy and intelligence practitioners, the lesson is that sovereignty in PNG has always been contested across multiple domains—political, economic, Military and social—and that safeguarding it requires both internal legitimacy and careful external diplomacy.

Chapter 2: Mapping the Shadows

Geopolitical Hotspots Affecting PNG

Papua New Guinea (PNG) occupies a strategically significant position in the Indo-Pacific, located between Southeast Asia, Australia, and the wider Pacific Island region. While PNG is not a primary kinetic conflict state, it is increasingly embedded within zones of geopolitical competition, strategic influence operations, and proxy economic warfare (Medcalf, 2020; Fry & Tarte, 2015). The convergence of great-power rivalry, maritime insecurity, resource competition, and border instability has transformed PNG into a secondary strategic theatre of contestation.

The South China Sea and Taiwan Strait

The South China Sea and Taiwan Strait represent the most volatile flashpoints in the contemporary international system (Allison, 2017; Mearsheimer, 2021). Any escalation between China, Taiwan, and United States-aligned forces would immediately disrupt Indo-Pacific trade, shipping lanes, and strategic stability.

For PNG, the impact is indirect but severe. The majority of PNG's fuel, manufactured goods, technology inputs, and maritime freight are dependent on shipping routes that pass through or near contested zones (Bateman & Bergin, 2019). Escalation would trigger:

- Supply chain disruptions
- Inflationary pressure on energy and food
- Foreign investment contraction
- Increased intelligence operations across Melanesia

Thus, although geographically removed, PNG is economically and strategically exposed to East Asian Military escalation.

United States–China Strategic Rivalry in the Pacific

The Pacific Islands region has shifted from a development-focused diplomatic space to an active geopolitical competition zone (Dibb & Brabin-Smith, 2017; Henderson & Reilly, 2021). Both China and the United States, along with allied partners, are now competing through:

- Infrastructure finance
- Technology systems
- Security cooperation
- Defence training and port access

This rivalry places PNG under strategic pressure to balance competing security and economic relationships. According to Powell (2020), such competition creates vulnerability to:

- Debt leverage
- Political elite capture
- Telecommunications surveillance exposure
- Dual-use infrastructure risk

PNG is no longer viewed as geopolitically peripheral; it is now framed as strategically pivotal within Melanesia.

Indonesian Papua (West Papua) Conflict Zone

PNG shares a long and porous land border with Indonesia's Papua provinces—one of the most militarized internal security zones in Southeast Asia (Webb-Gannon, 2014; King, 2016). This conflict presents PNG's most immediate physical geopolitical exposure.
Key spillover vulnerabilities include:

- Refugee movements
- Arms and narcotics trafficking
- Cross-border militia mobility
- Intelligence surveillance penetration
- Political activist mobilization across the border

May (2018) notes that PNG's historical non-intervention policy has not eliminated these risks, instead shifting them into informal and covert security channels. Border destabilization remains a persistent national security pressure point.

Solomon Islands and Pacific Militarization

Recent security agreements between external powers and the Solomon Islands have accelerated the normalization of Military presence in Melanesia (Dornan & Newton Cain, 2022). This shift has altered the strategic geometry of the South Pacific.
For PNG, this creates:

- Increased naval traffic in maritime approaches
- Intelligence activity around ports
- Strategic recalibration of PNG maritime space
- Regional power projection competition

This development has repositioned Melanesia from a security vacuum to a contested maritime arena (Bateman, 2022).

Australia–PNG Strategic Defence Axis

Australia remains PNG's primary defence and security partner. However, this relationship now operates within the context of broader Indo-Pacific deterrence architecture (White, 2019). While Australia provides:

- Training
- Intelligence cooperation
- Border security support

There is an accompanying risk of structural dependency, where national doctrine, intelligence systems, and strategic priorities become externally aligned. This relationship is stabilizing but also shapes PNG's strategic autonomy.

Maritime Southeast Asia Criminal Corridor

The Philippines–Indonesia–Malaysia maritime triangle remains a major route for:

- Illegal arms trafficking

- People smuggling
- Terror financing
- Narcotics movement

Transnational criminal syndicates utilize maritime routes extending into the Southwest Pacific (UNODC, 2021). PNG's ports, fisheries zone, and customs limitations create entry pathways for financial and physical security threats.

Global Resource Competition

PNG's wealth in:

- LNG
- Gold
- Copper
- Timber
- Fisheries
- Forestry

has placed it within zones of global resource geopolitics (Howes, Wira, & Swan, 2020). State-linked corporations, sovereign investment funds, and offshore intermediaries often operate at the boundary between commercial and strategic intent.

Risks include:

- Contract manipulation
- Royalty suppression
- Foreign economic leverage
- Corruption capture through commodity finance

Resource competition increasingly functions as a vector of hybrid geopolitical pressure (Klare, 2012).

Strategic Intelligence Assessment

PNG is situated within seven overlapping geopolitical pressure zones:

1. East Asian Military escalation risk
2. US–China Pacific rivalry
3. West Papua border insecurity
4. Melanesian militarization
5. Australia–PNG defence alignment
6. Transnational maritime crime corridors
7. Global resource competition

These forces converge not primarily through warfare, but through:

- Finance
- Infrastructure
- Cyber systems
- Political funding
- Intelligence influence operations

Core National Vulnerability

PNG's principal geopolitical vulnerability is not Military weakness, but:

- Institutional fragility
- Port and border insecurity
- Political finance exposure
- Economic dependency

These conditions form the primary entry points for external strategic influence.

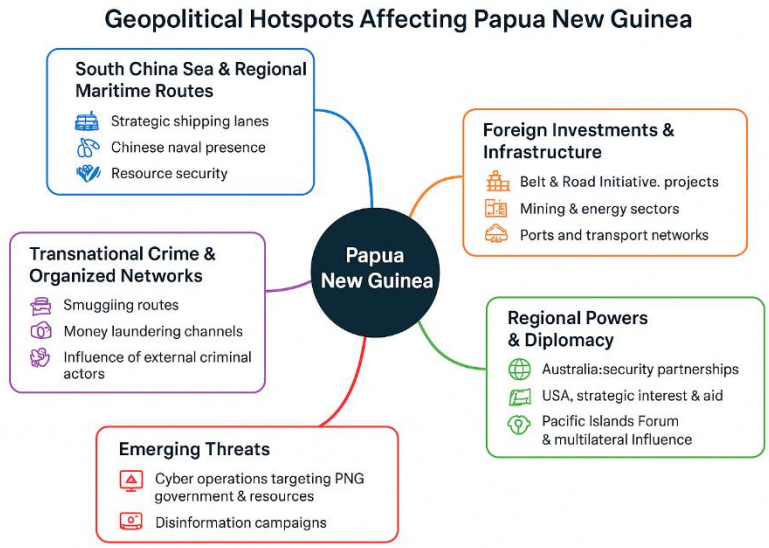

Geopolitical Hotspots Affecting Papua New Guinea
South China Sea & Regional Maritime Routes
Strategic shipping lanes
Chinese naval presence
Resource security
Foreign Investments & Infrastructure
Belt & Road Initiative. projects
Mining & energy sectors
Ports and transport networks
Papua New Guinea
Transnational Crime & Organized Networks
Smuggiing routes
Money laundering channels
Influence of external criminal actors
Regional Powers & Diplomacy
Australia:security partnerships
USA, strategic interest & aid
Pacific Islands Forum & multilateral Influence
Emerging Threats
Cyber operations targeting PNG government & resources
Disinformation campaigns

Diagram 4 Geopolitical Hotspots Affecting PNG

Chapter 3: Vulnerabilities Within

Critical Infrastructure Weak Points (Ports, Energy, Communications)

Critical infrastructure forms the backbone of national security, economic survival, and sovereign control. In Papua New Guinea (PNG), vulnerabilities within ports, energy systems, and communications networks represent not only technical weaknesses, but also strategic entry points for foreign influence, criminal penetration, and hybrid warfare (Medcalf, 2020; Dornan & Newton Cain, 2022). These systems are increasingly targeted globally as instruments of coercion, disruption, and geopolitical leverage rather than purely Military conquest.

Ports and Maritime Infrastructure

PNG's maritime domain is central to its economic and security survival. Over 90% of PNG's imports and exports move through seaports, including fuel, food, mining exports, and security equipment (Howes, 2020; UNCTAD, 2021). Yet many PNG ports face structural underinvestment, limited surveillance coverage, and fragmented security coordination.

Globally, ports are recognized as primary hybrid warfare targets, vulnerable to sabotage, smuggling infiltration, cyber compromise, and political coercion (Bateman & Bergin, 2019). In PNG, key weaknesses include:

- Limited real-time maritime domain awareness
- Inadequate container screening capacity
- Private–public security fragmentation
- Corruption exposure in customs and logistics chains

Dornan (2021) notes that port infrastructure in the Pacific is increasingly shaped by external financing and construction, which introduces foreign technical dependency and hidden data access risks. This creates vulnerabilities not only to criminal exploitation, but also to covert intelligence collection and strategic surveillance.

From a national security perspective, any disruption to PNG ports would rapidly:

- Paralyze fuel distribution
- Disrupt food security
- Halt mineral exports
- Degrade defence mobility

Thus, ports represent a systemic national vulnerability rather than a single-point failure risk.

Energy Infrastructure

Energy systems—particularly electricity generation and fuel supply chains—are among the most fragile components of PNG's infrastructure architecture. PNG's power grid remains regionally

fragmented, lightly protected, and highly concentrated in urban centers, especially Port Moresby and Lae (ADB, 2020; Howes et al., 2020).

International literature identifies energy infrastructure as a primary coercive target in modern conflict, where disruption achieves psychological, political, and economic shock without kinetic warfare (Klare, 2012; Mearsheimer, 2021). In PNG, vulnerabilities include:

- Dependence on imported refined fuel
- Limited strategic fuel reserves
- Single-point transmission failures
- Minimal redundancy in grid architecture

The LNG sector, while economically vital, also introduces strategic exposure through foreign capital concentration, offshore financial dependence, and cyber–industrial control vulnerabilities (Allen & Hasnain, 2019). Disruption—whether physical, cyber, or financial—would produce immediate national-level instability.

Communications and Digital Infrastructure

Communications infrastructure now constitutes the central nervous system of national power. Telecommunications, undersea cables, mobile networks, satellite services, and government data centers form the backbone of governance, defence coordination, emergency services, and economic activity.

Globally, communications systems are now targeted through cyber intrusion, data interception, disinformation injection, and infrastructure sabotage (Nye, 2018; Kello, 2017). In PNG, structural weaknesses include:

Limited cyber defence capacity

- Heavy reliance on foreign-owned network infrastructure
- Insufficient data sovereignty controls
- Low redundancy in international cable connectivity

Powell (2020) warns that Pacific states face increasing risks of digital capture, where state decision-making becomes indirectly shaped through control over digital platforms, payment systems, and information flows. In an intelligence context, compromised communications infrastructure becomes both a surveillance platform and a disruption weapon.

Strategic Intelligence Assessment

Across ports, energy, and communications, PNG's critical infrastructure weaknesses are shaped by three converging pressures:

- External capital dependency
- Institutional security capacity gaps
- Hybrid warfare convergence of financial, cyber, and physical threats

These vulnerabilities do not operate in isolation. A coordinated hybrid campaign could, for example, combine:

- Financial leverage on port operators
- Cyber interference in fuel logistics
- Disinformation targeting energy failures

Such convergence would produce national disruption without formal Military engagement.

PNG's critical infrastructure is not merely an economic concern—it is a primary national security battlefield of the 21st century. Ports enable sovereignty over trade. Energy enables state functionality. Communications enable command, control, and legitimacy. Weakness across any of these domains exposes PNG to coercion, disruption, and strategic manipulation by external and internal actors alike.

Without sustained protective investment, intelligence integration, and institutional hardening, critical infrastructure will remain the most accessible gateway for national destabilization.

Insider Threats: Corruption, Compromise, Human Factor

While external threats attract most national security attention, history consistently demonstrates that the most damaging breaches of critical infrastructure and state security originate from within. Insider threats—driven by corruption, compromise, coercion, ideology, financial stress, or personal grievance—represent the most persistent and least visible vulnerability in national systems (Shaw, Ruby, & Post, 2013; Kello, 2017). In fragile institutional environments, the human factor often becomes the primary attack surface.

In Papua New Guinea (PNG), insider threats are magnified by weak accountability mechanisms, economic inequality, political patronage networks, and limited counter-intelligence capacity, creating fertile ground for infiltration, data leakage, and system sabotage (Dornan & Newton Cain, 2022; Howes, 2020).

Corruption as a National Security Weapon

Corruption is no longer viewed solely as a governance failure—it is now widely recognized as a strategic national security weapon used by state and non-state actors to penetrate institutions, influence decision-making, and neutralize enforcement systems (Rose-Ackerman & Palifka, 2016; Medcalf, 2020).

In PNG, corruption affects multiple layers of state infrastructure, including:

- Customs and border control

- Ports and logistics
- Energy procurement
- Telecommunications licensing
- Law enforcement and regulatory agencies

Transparency International (2023) consistently identifies corruption as one of the most significant impediments to effective governance in PNG. From an intelligence perspective, corruption enables:

- Unrestricted access to secure facilities
- Manipulation of procurement and contracts
- Facilitation of smuggling and financial crime
- Suppression of investigations

This transforms corruption into a force multiplier for external actors, allowing them to bypass formal security architecture without triggering conventional threat indicators.

Compromise and Coercion of Personnel

Insider compromise rarely occurs through loyalty alone. Global intelligence research confirms that most compromised personnel are driven by financial distress, blackmail, ego, ideological sympathy, fear, or perceived injustice (Shaw et al., 2013; Lowenthal, 2020). PNG's socio-economic environment—characterized by cash pressures, extended family obligations, and limited institutional welfare—creates persistent exposure to coercive recruitment.

Compromise pathways commonly include:

- Debt exploitation

- Romantic entanglements
- Tribal and political loyalties
- Business inducements
- Threats against family members

In small institutional environments such as PNG's, once a single insider is compromised, entire systems can be rapidly mapped and penetrated due to overlapping personal networks and informal information sharing.

The Human Factor in Infrastructure and Security Systems

Even the most advanced infrastructure is only as secure as the human beings who operate it. The "human factor" remains the weakest link in cyber systems, physical security, and classified information handling (Nye, 2018; Kello, 2017). In PNG, this challenge is intensified by:

- Limited continuous vetting systems
- Irregular security clearance reinvestigations
- Weak lifestyle auditing
- Cultural reluctance to report colleagues

Fear of retaliation

Dornan (2021) notes that institutional resilience in the Pacific is constrained not by technical knowledge but by personnel integrity under pressure. This creates a persistent gap between formal security policy and operational reality.

Insider Threats and Hybrid Warfare

Modern hybrid warfare relies heavily on insider facilitation rather than overt attack. According to Medcalf (2020) and Mearsheimer (2021), contemporary power competition increasingly centers on:

- Subversion rather than invasion
- Co-option rather than conquest
- Influence rather than occupation

In this model, compromised insiders become strategic assets, enabling cyber incursions, logistics sabotage, intelligence theft, and political destabilization without attribution. For PNG, whose national systems remain heavily dependent on manual procedures and trust-based access, insider threats pose a disproportionate national risk relative to the size of the state.

Strategic Intelligence Implications for Papua New Guinea

From a national intelligence perspective, insider threats in PNG are driven by four reinforcing dynamics:

- Economic vulnerability of personnel
- Weak institutional enforcement
- High exposure to foreign capital and influence
- Low counter-intelligence penetration depth

These conditions allow hostile actors to pursue long-term quiet infiltration strategies, embedding themselves within infrastructure, regulatory agencies, and information systems without triggering conventional warning indicators.

Insider threats represent the most dangerous category of national security risk because they operate invisibly, exploit trust, and bypass technological safeguards. In PNG, corruption, compromise, and human vulnerability do not simply weaken governance—they directly erode sovereignty, intelligence integrity, and state control over critical systems.

Until insider threat management is treated as a core intelligence function rather than an administrative afterthought, PNG's critical infrastructure will remain structurally exposed from within.

Technology and Cybersecurity Gaps

In the modern security environment, cyberspace has become a primary domain of conflict, alongside land, sea, air, and space. States now experience sustained competition through cyber espionage, cyber sabotage, influence operations, data theft, and digital infrastructure disruption (Kello, 2017; Nye, 2018). For developing states such as Papua New Guinea (PNG), cyber vulnerability is not only a technical issue—it is a **strategic national security** exposure**.**

PNG's rapid digital adoption has not been matched by equivalent growth in cyber governance, infrastructure protection, technical workforce capacity, and intelligence integration**,** leaving wide gaps exploitable by hostile state and non-state actors (Dornan & Newton Cain, 2022; Asian Development Bank [ADB], 2021).

Structural Weaknesses in PNG's Cyber Architecture

PNG's national cyber posture remains fragmented and under-resourced**,** with cybersecurity responsibilities dispersed across multiple agencies without unified national command or integrated intelligence oversight. While policy intent exists, operational execution remains weak due to:

- Limited national cyber legislation enforcement
- Weak regulatory authority over Internet Service Providers
- Absence of a fully functional national Computer Emergency Response Team (CERT)
- Poor inter-agency information sharing
- Minimal offensive cyber intelligence capability

The ADB (2021) identifies PNG as one of the Pacific states with the lowest levels of cyber maturity, particularly in areas of cyber risk governance, threat intelligence, and incident response readiness.

Critical Infrastructure Cyber Exposure

PNG's critical infrastructure—including ports, power generation, telecommunications, aviation, banking, and government databases—has undergone rapid digitization without integrated cyber security hardening**.** According to Kello (2017), this creates a condition known as **"**strategic cyber fragility," where even minor intrusions can trigger cascading failures across national systems.

In PNG, major vulnerabilities include:

- Outdated software systems in government networks
- Weak access control protocols
- Limited encryption use
- Poor data backup discipline
- High dependency on foreign-managed platforms

Dornan (2021) notes that many Pacific states, including PNG, rely heavily on **foreign technical vendors for infrastructure maintenance**, creating **supply chain security risks and intelligence exposure**.

Human Capital and Technical Skill Deficits

Cyber security is not sustained by hardware alone—it is sustained by skilled human operators. PNG faces a chronic shortage of:

- Cyber security analysts
- Network defense specialists
- Digital forensics personnel
- Malware and intrusion analysts
- Cyber-intelligence officers

This shortage forces government agencies and corporations to depend on external contractors**,** significantly increasing the risk of data leakage, embedded vulnerabilities, and foreign surveillance (Medcalf, 2020; Lowenthal, 2020). The inability to independently audit systems undermines sovereign control of national data.

Cybercrime, Financial Systems, and State Vulnerability

Cybercrime increasingly intersects with national security through:

- Online financial fraud
- Cryptocurrency laundering
- Identity theft
- Banking intrusions
- Dark web trafficking

INTERPOL (2022) identifies cyber-enabled financial crime as one of the fastest-growing security threats in the Pacific. For PNG, whose financial systems support national revenue, salaries, and procurement, even limited cyber intrusion can create:

- Payroll system manipulation
- Revenue leakage
- Procurement fraud
- Institutional destabilization

These operations often rely **on** hybrid networks combining foreign cyber actors and local **compromised insiders**, blurring distinctions between crime and espionage.

Foreign Influence and Digital Dependence

Global strategic competition has extended into digital infrastructure diplomacy, where external powers compete through:

- Telecommunications infrastructure
- Subsea cable systems

- Data hosting services
- Satellite connectivity

Medcalf (2020) and Mearsheimer (2021) argue that digital dependence now constitutes a **geopolitical vulnerability equivalent to energy dependence**. For PNG, reliance on foreign digital architecture without independent cyber monitoring capability creates exposure to:

- Strategic surveillance
- Data interception
- Coercive leverage
- Infrastructure disruption during crises

Disinformation, Psychological Operations, and Social Media Threats

Cyber threats in PNG do not stop at infrastructure—they extend into psychological and informational domains. Social media platforms have become vectors for:

- Disinformation campaigns
- Social destabilization
- Electoral manipulation narratives
- Tribal and political incitement

Nye (2018) emphasizes that cyber power now enables mass influence without physical presence, allowing hostile actors to shape national perception at scale. PNG's fragmented information environment and high mobile phone penetration make it especially vulnerable to externally engineered narrative warfare**.**

Intelligence Gaps in Cyber Threat Detection

PNG's intelligence architecture remains heavily oriented toward traditional physical threats**,** with limited cyber-intelligence fusion. This creates blind spots in:

- Early detection of cyber intrusion
- Attribution of cyber attacks

- Monitoring of foreign cyber reconnaissance
- Hybrid operations linking cyber and physical threats
-

Without integrated cyber-intelligence capability, cyberattacks in PNG risk being misclassified as **technical failures rather than hostile operations**, delaying national response.

Strategic Security Implications

From a national security perspective, PNG's cyber gaps generate five major strategic risks:

1. Loss of sovereign control over national data
2. Systemic exposure of critical infrastructure
3. Financial destabilization through cybercrime
4. Foreign intelligence penetration through digital systems
5. Psychological influence operations against the population

These risks do not operate independently—they reinforce each other, creating a layered strategic vulnerability environment**.**

Technology and cyber security gaps now represent a core national security vulnerability for Papua New Guinea**.** The convergence of weak infrastructure protection, limited cyber-intelligence capability, foreign digital dependence, and rising cyber-enabled crime creates a condition in which hostile actors can project power into PNG without deploying a single soldier**.**

Until cyber security is treated as a strategic intelligence function rather than a purely technical service, PNG will remain exposed to silent, persistent, and deniable cyber conflict operations.

Lessons from Previous Security Breaches

Case Study

Black Wednesday

January 10th 2024

Black Wednesday on primarily a domestic socioeconomic–political unrest event with hybrid elements.

Reasoning: the immediate trigger was a protest by police, corrections and other public-sector officers over sudden payroll deductions and rumours about new taxes — a domestic grievance that escalated into looting, arson and widescale unrest. However, the incident exhibited hybrid characteristics (information/misinformation spread, possible political manipulation, coordinated opportunism, and targeting of economic actors) that amplified its impact beyond a simple strike. The government itself described elements of the unrest as "organised," and inquiries were launched to examine capacity, organization and possible outside influences.

Why it reads as part domestic, part hybrid

The core grievance was economic: payroll deductions and perceived policy changes triggered the initial protest by security personnel; that made the unrest organic and domestic.

Hybrid features appeared because social media and rumours amplified anger and spread misinformation quickly, opportunistic actors exploited disorder for looting, and political actors/interest groups may have steered or benefited from instability (the PM said "deep political influence" was involved). These mixed modalities (social, political, criminal) are characteristic of hybrid incidents.

The targeting of Chinese businesses and major commercial centres and coordinated damage/looting suggests some actors moved from protest into instrumentalized, organised economic violence — a sign that the unrest had moved beyond spontaneous protest.
Wikipedia

What could have been done to STOP or blunt the occurrence — practical, intelligence-grade measures

Preventive measures (short-term / pre-event)

Immediate payroll integrity checks and rapid public correction: When pay anomalies appeared, the government needed a transparent, rapid, clearly worded public correction and immediate interim

relief (emergency top-up payments) to remove the grievance trigger. A single credible corrective action within hours reduces the acute anger vector.

Targeted engagement with security personnel leaders: Senior leaders (police, corrections, Military) should have been rapidly engaged in private—listening, offering interim remedies, and securing commitment to non-violence. When the protesting cohort included security personnel, the risk of escalation multiplies.

Rapid counter-misinformation campaign: Centralised, verified messaging (radio, TV, SMS blasts into affected provinces) to counter rumours about taxes/pay changes and to provide clear instructions about lawful grievance channels. In PNG contexts where word-of-mouth dominates, rapid authoritative messaging is essential.

Dampening measures (hours → days)

Deploy pre-planned surge policing with strict ROE and community liaison: A coordinated deployment of disciplined units trained in crowd control and community protection — not heavy-handed retaliatory tactics that inflame crowds. Clear rules of engagement, accompanied by community mediators, reduce civilian casualties and prevent the narrative of state repression.

Protect key commercial/critical infrastructure proactively: Pre-identification and guarded protection of high-risk sites (markets, central shopping centres, ports, Chinese-owned businesses) and secure evacuation routes for civilians could have limited looting and mass losses.

Emergency economic relief and targeted cash assistance: Short-term cash relief (even modest) to the worst-affected communities lowers incentives for opportunistic looting and reduces recruitment into violent acts. International partners can pre-position assistance agreements for rapid disbursement.

Longer-term systemic measures (weeks → years)

Fix payroll systems & improve administrative resilience: Audit and harden payroll/financial admin systems (redundant checks, rollback procedures, emergency top-ups) so “technical glitches” cannot instantly become political crises.

Strengthen grievance channels and union/leadership engagement: Institutionalize safe, transparent channels for security and public-sector employees to air and resolve pay/benefit disputes. Preventing mass public strikes depends on credible internal arbitration.

Improve civil-Military/police relations & oversight: Strengthen accountability, training, and oversight so that when security personnel protest, they do not weaponize public trust or cause vacuums that others exploit. Independent inquiry and reforms post-event are necessary to rebuild trust.

Community resilience & early-warning networks: Build grassroots reporting and local mediation capacity (churches, ward leaders, market committees) to detect grievances before they boil over and to mediate locally. Devpolicy and ANU analyses highlight community-level drivers and the need for localized responses.

Threat indicators that should have raised alarm (actionable list for intel/ops)

- Operational teams should watch both direct and amplifier indicators:
- Direct indicators (immediate operational risk)
- Sudden, coordinated withdrawal or mass absence of security personnel from duty (police/Military/corrections)
- Payroll anomalies, mass complaints about pay, or simultaneous official HR notifications affecting thousands
- Organised mass gatherings of uniformed/security personnel near government precincts or parliament
- Rapid spread of calls to protest on local radio, SMS chains, and messaging apps
- Amplifier indicators (information & opportunist risks)
- Spikes in social media rumours (taxation changes, pay cuts), or coordinated hashtags/messages across channels

- Sudden mobilization of youth gangs or known criminal networks into protest areas

- Signs of coordination for looting (e.g., groups pre-positioning transport, reported directions to hit commercial nodes)

- Targeting patterns (e.g., repeated attacks against specific ethnicity-owned shops or foreign nationals' businesses) indicating bias or political/ethnic profiling

- Chatter suggesting political actors are seeking to steer the unrest or promising impunity to looters (would show up in HUMINT or open-source monitoring)

Intelligence value of combining indicators

Any combination of payroll anomalies + withdrawal of security personnel, combined with rapid social-media amplification should trigger an elevated threat posture and immediate protective action. The "hybrid" risk is visible when the amplifier indicators are present alongside a genuine grievance: the crisis becomes both legitimate and exploitable.

Short analytical summary / realistic assessment

Black Wednesday began as a legitimate domestic grievance (pay glitches and tax rumours) but morphed into a national crisis because structural vulnerabilities (weak payroll governance, limited immediate communication channels, under-resourced crowd control & protection of commercial nodes) and opportunistic actors turned grievance into violent opportunism. The hybrid risk profile was created by the mix of social amplification, opportunistic criminality, and possible political exploitation. That combination made a rapid localized strike escalate into a national security emergency.

Chapter 4: Intelligence Collection and Analysis

OSINT in the Papua New Guinea Context

Open-Source Intelligence (OSINT) has become one of the most accessible and rapidly expanding intelligence disciplines in Papua New Guinea due to the nation's widespread mobile phone use, the growth of online news platforms, and the increasing presence of social media accounts across provinces. In PNG, OSINT supports both Military and police operations by enabling collection from publicly available sources such as Facebook community pages, local news outlets, TikTok videos from conflict zones, and citizen reporting during emergencies.

Because PNG lacks the advanced surveillance platforms used by larger states, OSINT serves as a force multiplier. During tribal conflicts, for example, photos and videos uploaded by civilians often provide the first indicators of mobilization, weapon displays, roadblocks, or rumours of payback killings. OSINT also contributes to national security by tracking foreign influence, organized criminal networks, and external actors using public corporate registers, vessel tracking data, or international media reports.

However, PNG's OSINT environment is complicated by misinformation, political propaganda, and low digital literacy. Analysts require strong verification skills—triangulating sources, geolocating images, cross-checking timestamps, and evaluating authenticity. International best practice encourages structured OSINT processes: defining collection requirements, applying ethical guidelines, protecting personal data, and ensuring analysts do not expose themselves to counter-surveillance online (Rid & Buchanan, 2015).

Ultimately, OSINT provides PNG security agencies with high-value, low-cost intelligence that complements more sensitive collection disciplines and helps overcome geographic and logistical barriers.

HUMINT: Handling Sources Safely

Human Intelligence (HUMINT) remains the cornerstone of intelligence work in PNG, especially given the country's relational culture, clan-based networks, and the need for on-the-ground insights into local grievances, criminal activity, and foreign influence. HUMINT is effective because trusted

community intermediaries often possess unique insights that technical sensors cannot detect, such as intentions, loyalties, or internal disputes within groups.

Safe source handling is critical. PNG's social environment—marked by wantok obligations, land disputes, and inter-tribal relationships—creates risks of exposure, retaliation, and compromised confidentiality. Agents and informants may be vulnerable to coercion by criminal groups, political actors, or foreign networks seeking control. Handling protocols require:

- rigorous vetting of sources to assess credibility, motivation, and risk
- secure meeting locations and communication channels
- careful management of payments or incentives to prevent dependency
- maintaining psychological safety and confidentiality
- documenting interactions and avoiding personal entanglements
-

Global HUMINT doctrine emphasizes rapport building, cultural fluency, and ethical constraints to prevent coercion or manipulation (Fishbein & Treverton, 2019). PNG's experience indicates that HUMINT is most effective when collectors understand local power dynamics, respect community protocols, and avoid actions that could unintentionally escalate conflict.

SIGINT and Emerging Technologies

Signals Intelligence (SIGINT) is increasingly relevant to PNG's national security landscape as mobile networks, messaging apps, and digital communication tools become widespread. Although PNG does not currently have large-scale interception capabilities like those of Australia or the United States, targeted SIGINT operations support investigations into transnational crime, cyber-enabled fraud, and foreign interference.

Emerging technologies—such as AI-powered text analysis, pattern-of-life mapping, and metadata exploitation—enable agencies to detect abnormal communication spikes, coordinated online behaviour, or encrypted messaging patterns linked to organized crime groups. Satellite-based monitoring, including AIS (Automatic Identification System) signals, improves maritime domain awareness, particularly against illegal fishing and unreported vessel movements in PNG's vast Exclusive Economic Zone.

Challenges include limited technical infrastructure, reliance on foreign partners, and the legal mandate required for interception activities. Ensuring constitutional compliance, data privacy, and judicial oversight is essential to maintain public trust and prevent abuse.

Other Intelligence Types and PNG's Need for Development

Modern intelligence ecosystems rely on multiple collection disciplines. Beyond OSINT, HUMINT, and SIGINT, PNG can benefit from developing additional capabilities used widely around the world: GEOINT (Geospatial Intelligence) – Uses satellite imagery, drone reconnaissance, and mapping tools to analyse terrain, population movements, and conflict patterns. GEOINT is valuable for natural disaster response, border monitoring, and assessing illegal mining in remote regions.

TECHINT (Technical Intelligence) – Examines foreign equipment, weapons, communications tools, and emerging technologies used by adversaries. PNG could apply TECHINT to analyse seized weapons, improvised explosive devices, or smuggling methods used by transnational crime groups. MASINT (Measurement and Signature Intelligence) – A highly specialized field analysing physical signatures such as radiation, chemicals, acoustics, or electromagnetic anomalies. While advanced, elements of MASINT can support PNG's environmental monitoring, resource protection, and maritime surveillance.

FININT (Financial Intelligence) – Tracks money flows, shell companies, foreign financial interference, and corruption networks. Given PNG's vulnerability to money laundering and organized crime, FININT partnerships with financial institutions and global regulators are essential. Building multi-disciplinary intelligence capabilities requires investment, training, legal frameworks, and integration across agencies to ensure a unified national intelligence architecture.

Analysis Tools: Threat Assessment Models and Probabilities
Effective threat assessment transforms raw intelligence into actionable understanding. Analysts evaluate intent, capability, opportunity, and indicators to determine the probability of threats materializing. Widely used models include:

- The Intelligence Cycle – tasking, collection, processing, analysis, dissemination

- Structured Analytic Techniques – such as red teaming, competing hypotheses, and scenario analysis (Heuer & Pherson, 2014)
- Risk Matrix Models – plotting likelihood against impact to classify threat severity
- Pattern and Trend Analysis – identifying behavioural signatures, escalation pathways, or seasonal spikes in violence
- Predictive Modelling – using probabilities to forecast attacks, foreign influence campaigns, cyber intrusions, or tribal conflict outbreaks

In PNG, threat assessment models must incorporate localized variables such as clan alliances, election cycles, resource tensions, land ownership disputes, and foreign commercial activities. Analysts should combine quantitative data (crime statistics, communication metadata, financial patterns) with qualitative insights (community reports, HUMINT narratives, OSINT trends) to produce balanced assessments.

Accurate threat estimation supports command decision-making, resource allocation, and proactive disruption of hostile activities. When analysts adhere to structured methodologies rather than intuition alone, they reduce cognitive bias and strengthen the reliability of national intelligence efforts.

- Open-Source Intelligence (OSINT) in PNG Context
- Human Intelligence (HUMINT): Handling Sources Safely
- Signals Intelligence (SIGINT) and Emerging Technologies
- Analysis Tools: Threat Assessment Models and Probabilities

Chapter 5: External Actors' Methods and Tactics

Cyber Operations and Digital Espionage

Cyber operations and digital espionage have become central instruments in the methods and tactics of external actors seeking to influence, exploit, or destabilize states without crossing the threshold of conventional Military conflict. Unlike traditional espionage conducted through physical infiltration, cyber-enabled espionage operates across invisible networks, targeting government systems, critical infrastructure, economic institutions, and civilian populations simultaneously. The low cost of entry, high deniability, and global reach of cyber operations make them one of the most effective asymmetric tools in modern hybrid warfare (Kello, 2017; Rid, 2020).

External actors employ cyber operations for a wide spectrum of strategic objectives. These include the theft of classified government information, surveillance of political leaders, disruption of essential services, economic espionage targeting trade and resource sectors, manipulation of public opinion through information operations, and long-term positioning inside national digital infrastructure for future coercive leverage (Clarke & Knake, 2019). Unlike kinetic attacks that generate immediate visibility, cyber operations often remain undetected for months or years, allowing adversaries to extract intelligence continuously while shaping the strategic environment covertly.

Digital espionage relies heavily on layered intrusion techniques. These include phishing campaigns, malware implants, zero-day exploits, supply-chain attacks, credential harvesting, and insider compromise. State-sponsored actors frequently use Advanced Persistent Threat (APT) groups to maintain long-term access to targeted systems. These groups demonstrate high levels of discipline, technical sophistication, and operational patience, often embedding themselves within networks until strategic timing dictates activation (Bejtlich, 2013; FireEye, 2022).

Information warfare is closely intertwined with cyber espionage. External actors increasingly combine hacking with psychological operations designed to manipulate narratives, erode public trust, incite social division, and undermine confidence in state institutions. Disinformation campaigns targeting elections, public health, law enforcement, and national leadership have become a defining feature of the modern threat environment (Wardle & Derakhshan, 2017). These operations are particularly effective in environments where digital literacy is uneven and trust in institutions is already strained.

For Papua New Guinea and similar developing digital states, cyber vulnerability is amplified by rapid digital adoption without proportional security investment. Government networks, banking systems, telecommunications providers, port operations, mining companies, and electoral infrastructure all rely increasingly on networked systems that remain unevenly protected. External actors exploit outdated software, weak authentication protocols, limited cyber training, and fragmented institutional coordination to establish footholds for espionage and economic exploitation (UNODC, 2021; Commonwealth Telecommunications Organisation, 2020).

Digital espionage also plays a central role in economic coercion. External actors target confidential trade negotiations, mining contracts, petroleum exploration data, fisheries licensing systems, and sovereign infrastructure agreements. By accessing these digital assets, hostile actors gain leverage over national economic decision-making, weaken bargaining positions, and sometimes manipulate markets in ways that benefit foreign strategic interests (Farrell & Newman, 2019). In resource-rich states such as Papua New Guinea, cyber-enabled economic espionage represents a direct threat to sovereignty and equitable development.

Maritime and border security are also increasingly digitized, making them vulnerable to cyber compromise. Vessel tracking systems, customs databases, biometric identity platforms, and immigration controls depend on network integrity. External manipulation of such systems enables illegal fishing, smuggling, human trafficking, weapons movement, and covert logistics operations. Cyber intrusion into these platforms therefore produces direct physical-world security consequences (Kello, 2017; UNODC, 2021).

Cyber operations further enable intelligence preparation of the environment. External actors map national digital terrain long before overt crisis emerges. They identify key nodes within communications networks, power grids, fuel systems, and financial platforms. During political unrest, natural disasters, or Military tensions, these pre-positioned accesses can be activated to disrupt services, paralyze response coordination, and magnify chaos. This form of strategic cyber pre-positioning represents a hidden battlespace beneath everyday civilian life (Rid, 2020).

Attribution remains one of the most difficult challenges in digital espionage. External actors route attacks through global proxy servers, compromised civilian devices, and criminal infrastructure to obscure responsibility. This layered deniability complicates diplomatic response, legal retaliation, and

deterrence. Even when attribution is technically strong, political attribution may remain constrained by international norms, strategic risk calculations, or evidentiary limitations (Clarke & Knake, 2019).

Cyber operations also intersect with insider threat dynamics. External actors frequently cultivate insiders within government agencies, telecommunications companies, banks, and infrastructure operators to gain credentials and bypass technical defenses. These insiders may be recruited through coercion, financial inducement, ideological alignment, or intimidation. In fragile institutional environments, insider compromise can be more damaging than technical hacking because it erodes trust within the security architecture itself (Bejtlich, 2013).

Effective defense against digital espionage therefore requires more than technology. It demands legal frameworks that support cyber investigations, inter-agency coordination between intelligence, telecommunications regulators, police, and Military cyber units, and consistent workforce development. Cyber security is not solely an IT function; it is an intelligence discipline that integrates technical forensics, counterintelligence, strategic warning, and foreign policy decision-making (Gill & Phythian, 2018).

Regional cooperation is also essential. Cyber threats do not respect maritime boundaries or airspace. External actors often route attacks across multiple Pacific and Southeast Asian networks before reaching their targets. Information sharing, joint cyber exercises, mutual legal assistance, and shared threat databases significantly enhance collective security resilience across the region (Commonwealth Telecommunications Organisation, 2020).

Ultimately, cyber operations and digital espionage represent a quiet but expanding battlespace where sovereignty is contested daily below the threshold of armed conflict. For Papua New Guinea, the strategic danger is not only that data may be stolen, but that national decision-making, economic sovereignty, electoral confidence, and public trust may be silently manipulated. External actors no longer need to land troops to shape outcomes; they only need persistent access to digital ecosystems that connect state, economy, and society.

In this sense, cyber defense must be understood as a core national security function equivalent to territorial defense, border control, and intelligence operations. Failure to secure the digital domain produces invisible vulnerabilities that adversaries will exploit when physical confrontation becomes

strategically inconvenient. The future of national security will therefore be decided as much in server rooms and encrypted networks as on land, sea, and air.

Influence Operations and Social Manipulation

Influence operations and social manipulation have become some of the most powerful non-kinetic tools used by external actors to shape political outcomes, weaken national cohesion, and distort public trust without triggering direct confrontation. Unlike conventional propaganda, modern influence operations operate through layered psychological, cultural, economic, and digital mechanisms designed to subtly guide perception, behavior, and loyalty over time (Wardle & Derakhshan, 2017; Rid, 2020). These operations thrive in open societies, digitally connected populations, and politically polarized environments.

At the core of influence operations is the strategic targeting of identity, grievance, fear, and aspiration. External actors study social fault lines such as ethnicity, class, religion, land ownership, corruption, youth unemployment, and governance credibility. These vulnerabilities are then exploited through emotionally resonant messaging that amplifies perceived injustice and delegitimizes state authority (Kaldor, 2012). Social manipulation does not invent conflict from nothing; it intensifies existing social tension and accelerates fragmentation.

Digital platforms have become the primary battlespace for influence operations. Social media algorithms reward emotionally charged content, enabling external actors to scale manipulation at minimal cost. Disinformation, misinformation, selective truth framing, and psychological nudging now operate continuously across Facebook, TikTok, WhatsApp, Telegram, and other platforms commonly used across the Pacific (Wardle & Derakhshan, 2017). Through coordinated inauthentic behavior, bot networks, proxy influencers, and anonymous pages, adversaries shape narratives without visible attribution.

Influence operations are also heavily localized. Messaging is linguistically adapted, culturally embedded, and socially contextualized to avoid detection. In Papua New Guinea, where oral communication, clan networks, and church influence remain central, social manipulation frequently spreads through respected individuals rather than anonymous accounts (Dinnen, 2001; Gelu, 2013).

External actors exploit this by cultivating community-level intermediaries who become unwitting amplifiers of strategic narratives.

Political processes are prime targets for influence operations. Elections, parliamentary motions, court decisions, land negotiations, and national development projects all attract foreign narrative shaping. External actors may not seek to install a specific leader but rather to maintain sustained political uncertainty, erode faith in democratic systems, and normalize instability (Rid, 2020). Yet overt regime change is not always the goal; long-term influence often yields greater strategic leverage than rapid disruption.

Religious and cultural channels are also vulnerable to manipulation. Faith-based authority carries enormous persuasive power in many societies, including PNG. External actors exploit this by embedding narratives within moral, salvation, unity, or threat discourses. Once politicized, religious language becomes a powerful vehicle for mobilization, fear conditioning, and obedience override (Gelu & Axline, 2008).

Influence operations also intersect tightly with cyber operations. Data harvested through digital espionage enables precise micro-targeting. Personal fears, financial stress, online habits, and social affiliations become predictive tools for psychological modeling. The fusion of cyber intelligence and behavioral science represents a new generation of strategic influence capability (Clarke & Knake, 2019).

Countering influence operations requires institutional coordination across intelligence agencies, media regulators, education systems, cyber authorities, and civil society. Influence warfare is not defeated solely by censorship or arrests. It is mitigated by public trust, media literacy, transparent governance, and credible leadership (Putnam, 2000; Gill & Phythian, 2018). Where citizens trust institutions, manipulation fails to take root.

For Papua New Guinea, influence operations represent a long-term strategic risk because of high mobile phone penetration, uneven media regulation, political volatility, and deep communal networks. Failure to understand and counter this form of warfare risks allowing external actors to shape national identity from within without firing a single shot.

Covert Funding and Smuggling Networks

Covert funding represents one of the most strategically dangerous tools used by external actors because it invisibly reshapes political behavior, social influence, and economic dependency without overt coercion. Money functions as an amplifier of influence, enabling the penetration of political parties, activist groups, media organizations, churches, civil society groups, business networks, and even security-related actors (Farrell & Newman, 2019). When funding streams are hidden, accountability collapses and sovereignty becomes structurally compromised.

Covert funding operates through multiple vectors: foreign shell companies, informal remittance channels, cash couriers, digital payment systems, cryptocurrency platforms, trade-based money laundering, infrastructure sponsorships, and corrupt procurement pipelines (UNODC, 2021; APG, 2020). These systems blur the boundary between legal investment and strategic manipulation. Financial flows that appear commercial may in fact serve geopolitical objectives.

The political dimension of covert funding is especially corrosive. External sponsors can influence candidate selection, policy positions, parliamentary voting behavior, regulatory enforcement, and national development priorities without public scrutiny. Once elected officials become financially dependent on foreign backers, their loyalty subtly shifts from national interest to sponsor interest (Bruneau & Boraz, 2007).

Covert funding also fuels social manipulation by sustaining activists, protest movements, militant labor actions, digital influencers, and community power-brokers. These actors may not be ideological agents of external powers, but financial dependency gradually aligns their messaging, timing, and escalation patterns with sponsor objectives (Rid, 2020). In fragile states, even modest funding can dramatically alter the balance of influence within communities.

In Papua New Guinea, the vulnerability to covert funding is increased by weak financial oversight, limited forensic accounting capacity, and high levels of informal economic circulation. The Asia/Pacific Group on Money Laundering has repeatedly identified PNG as high-risk for trade-based money laundering, corruption, and illicit financial movement (APG, 2020). Such financial invisibility enables foreign actors to embed influence inside political and social ecosystems with minimal resistance.

Resource-sector corruption represents a critical conduit for covert influence. Mining, petroleum, logging, fisheries, and infrastructure projects involve massive capital flows that attract foreign strategic interest. When licensing, royalties, land compensation, and regulatory enforcement are compromised by concealed foreign financial leverage, national sovereignty becomes structurally weakened (Dinnen, 2001).

Covert funding also intersects with cyber-enabled financial crime. Digital wallets, online gambling networks, crypto exchanges, and phishing-derived capital allow influence campaigns to self-finance through criminal revenue streams while appearing politically organic (Kello, 2017).

Countering covert funding requires integration of financial intelligence with national security strategy. Financial intelligence units, banking compliance systems, trade monitoring authorities, tax offices, procurement agencies, and border enforcement must operate as a unified intelligence network rather than isolated regulators (UNODC, 2021; Gill & Phythian, 2018).

For Papua New Guinea, defending against covert funding is not solely about financial integrity; it is about preventing the quiet purchase of national decision-making. Influence funded invisibly is influence that cannot be democratically resisted.

Case Studies: Lessons from Asia-Pacific Threat Actors

The Asia-Pacific region provides some of the most instructive contemporary case studies in hybrid threat behavior due to its convergence of great-power competition, fragile states, digital expansion, and contested maritime zones. These cases demonstrate how influence operations, covert funding, cyber operations, and social manipulation operate as integrated tools rather than isolated tactics (Kaldor, 2012; Rid, 2020).

In Southeast Asia, repeated cyber-enabled espionage campaigns against government ministries, energy companies, and electoral systems demonstrate how digital penetration precedes political pressure. Several states have experienced long-term access to their strategic databases without immediate disruption, only to face sudden policy destabilization during election cycles or trade negotiations. This

reflects cyber pre-positioning doctrine, where infrastructure is mapped long before overt pressure is applied (Kello, 2017).

In the South China Sea region, information warfare has operated alongside maritime coercion. Civilian fishing fleets, maritime militias, legal narratives, and diplomatic messaging are synchronized to normalize contested behavior. Social media campaigns inside targeted states gradually shift public perception toward acceptance of external claims, demonstrating influence operations as territory-shaping tools rather than merely opinion shaping (Clarke & Knake, 2019).

Pacific Island states increasingly experience infrastructure-based influence. Ports, roads, telecommunications towers, power grids, and government buildings funded externally often include opaque contractual terms. These projects establish economic leverage, intelligence access, and political dependency simultaneously (Firth, 2018). Once embedded, strategic pressure can be applied subtly through financing conditions rather than Military force.

In Melanesia, episodes of civil unrest linked to economic grievance, political dispute, and foreign commercial interest demonstrate how social instability can be amplified by hidden financial flows and narrative manipulation. The January 2024 unrest in Papua New Guinea illustrated how domestic triggers can be rapidly escalated into national crises when compounded by digital rumor warfare, criminal opportunism, and institutional strain (Dinnen & Allen, 2016).

Across the Asia-Pacific, the most consistent lesson is that modern threat actors rarely rely on one method alone. Cyber operations collect intelligence. Covert funding sustains influence. Social manipulation destabilizes identity. Economic leverage enforces compliance. Military presence then becomes unnecessary unless resistance emerges (Rid, 2020).

For Papua New Guinea, these cases demonstrate that national security can no longer be defined purely through defense forces and border patrols. The real battlespace now includes finance, media, cyberspace, diplomacy, religion, youth culture, land governance, and digital infrastructure. The adversary does not arrive in uniform. The adversary arrives as investment, partnership, activism, opportunity, and narrative.

The strategic lesson for PNG is therefore clear: hybrid threat defense must be anticipatory, not reactive. Sovereignty today is eroded gradually through influence rather than seized suddenly through invasion.

States that fail to recognize this shift become strategically owned before they realize they are under attack.

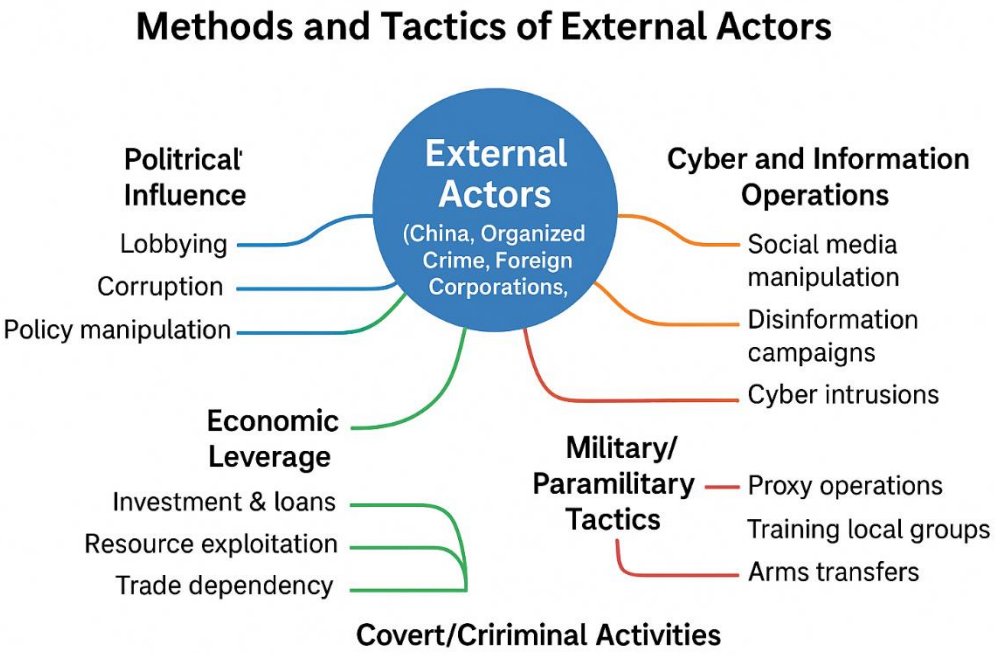


Diagram 5: Methods and Tactics of External Actors

Chapter 6: National Security Policy and Preparedness

PNG's Security Framework: Legal and Operational Overview

Papua New Guinea's national security architecture is built upon constitutional mandates, statutory legislation, regional agreements, and evolving operational practices shaped by historical experience and contemporary threat environments. These layers collectively inform how the state manages defence, intelligence, policing, and crisis preparedness. The most significant foundation is the Constitution of the Independent State of Papua New Guinea, which positions national security within the framework of democratic accountability and rule of law.

The Constitution sets out the roles and limits of core security institutions. Section 197 establishes the National Intelligence Organization (NIO), tasking it with collecting and analyzing intelligence relevant to national stability. The NIO's mandate includes monitoring espionage, sabotage, subversion, terrorism, and foreign interference. Section 202 outlines the functions of the Royal Papua New Guinea Constabulary (RPNGC), assigning responsibility for preserving peace, preventing crime, and enforcing the law. Section 205 establishes the Papua New Guinea Defence Force (MILITARY), which is responsible for the defence of the nation, supporting civil power when required, and responding to external aggression or major internal crises.

These constitutional provisions are complemented by key legislation. The National Intelligence Organization Act 1984 provides the specific legal basis for intelligence operations, including authorization processes, secrecy obligations, and ministerial oversight. The Defence Act 1974 governs force deployment, command structures, discipline, aid-to-civil-power arrangements, and operational conduct. The Police Act 1998 organizes command hierarchy, police powers, and investigative authority. The Emergency Act 1977 outlines executive powers during declared emergencies, including curfews, movement restrictions, and rapid mobilization of defence assets. The Cybercrime Code Act 2016 provides a legal foundation for investigating digital threats, cyber fraud, and foreign cyber interference—areas of growing concern as PNG's digital footprint expands.

Operationally, PNG's security framework operates through a mosaic of institutions that must collaborate closely to manage overlapping responsibilities. The National Security Council (NSC) functions as the apex decision-making body for high-level security matters, integrating assessments from the NIO, MILITARY, RPNGC, and the Department of Prime Minister & NEC. The Joint

Forces Headquarters (JFHQ) coordinates Military operations, while the National Disaster Centre (NDC) leads humanitarian and emergency responses. Interagency task forces—such as those addressing illegal fishing, smuggling, drug trafficking, and election security—bridge operational divides and enable joint action.

PNG's strategic environment requires a flexible and adaptive security framework. Internal instability such as tribal conflict, election-related violence, and high levels of violent crime remain persistent threats. External pressures include increasing competition among major powers in the Pacific, resource extraction disputes, porous borders, and the activities of foreign criminal networks. The legal and operational framework is therefore evolving toward more integrated models of security governance, but still faces limitations including inconsistent funding, political intervention, lack of fusion intelligence systems, and limited technological capabilities.

Strengthening PNG's security architecture will require investment in coordination mechanisms, modernization of legislation, development of secure communications systems, and consistent strategic planning. These reforms would bring PNG closer to global best practice while remaining grounded in the political, cultural, and geographic realities of the country.

Coordination Between Agencies and Military Intelligence

Effective national security in Papua New Guinea depends on the ability of state agencies to coordinate intelligence, operations, and strategic planning. PNG's threat environment—marked by a mix of tribal conflicts, transnational crime, political instability, natural disasters, and foreign geopolitical competition—demands an integrated approach. However, historical fragmentation between agencies remains one of PNG's most significant weaknesses.

Military Intelligence within the MILITARY plays a central role in assessing defence-related threats, monitoring the activities of foreign actors, analysing border security issues, and supporting joint operations. Meanwhile, the NIO provides strategic-level intelligence across political, economic, and security domains. The RPNGC focuses on criminal intelligence, including gang movements, organized crime networks, and domestic threat actors. Customs and the Immigration and Citizenship Authority contribute border and travel data, while the Financial Analysis and Supervision Unit (FASU) supports financial intelligence efforts. Despite their individual strengths, the absence of

standardized communication systems and shared reporting structures often leads to siloed information and operational confusion.

Coordination challenges are rooted in several factors: limited access to secure communication platforms, inconsistent interagency meetings, unclear mandates, and political sensitivities surrounding intelligence-sharing. Agencies may fear losing control of information, while others struggle with resource shortages that limit their ability to participate in joint initiatives.

International best practices suggest several pathways to improved coordination. First, establishing Joint Intelligence Committees (JICs) at both national and regional levels would create structured platforms for fusing intelligence streams. Second, adopting a common intelligence reporting format would standardize assessments and reduce ambiguity. Third, embedding liaison officers across agencies—especially between MILITARY, NIO, RPNGC, and Customs—would facilitate daily communication. Fourth, improving digital security infrastructure is essential, as the lack of encrypted systems often forces agencies to rely on informal networks.

PNG has made progress in certain areas. Election security operations increasingly involve integrated planning between RPNGC and MILITARY. Maritime operations against illegal fishing bring together Defence, Fisheries, NIO, and foreign partners. Border security patrols, especially along the Indonesian frontier, require Military-police coordination supported by village-level intelligence networks. These examples demonstrate that coordination improves significantly when tasking is clear and operational objectives align.

To further strengthen cooperation, PNG should consider developing a National Intelligence Fusion Centre, similar to models used in Australia, the United States, and the United Kingdom. Such a centre would centralize data, streamline analysis, reduce duplication, and produce unified threat assessments for the NSC. More importantly, it would ensure that MILITARY Military Intelligence receives timely civilian intelligence, and vice versa, enabling faster and more precise crisis responses.

Ultimately, fostering a culture of trust, accountability, and shared purpose across agencies will be the determining factor in elevating PNG’s national security posture. Modern threats no longer respect institutional boundaries, and PNG’s security institutions must adapt accordingly.

Crisis Response and Contingency Planning

Crisis response in Papua New Guinea requires a comprehensive, adaptive, and culturally informed framework due to the country's complex terrain, dispersed population, fragile infrastructure, and high exposure to both natural and human-induced threats. Effective contingency planning ensures that security institutions can anticipate crises, organize resources, and execute a rapid, coordinated response to minimize loss of life, protect critical assets, and preserve national stability.

PNG faces some of the highest disaster risks in the world—from earthquakes and volcanic eruptions to floods, landslides, and cyclones. These natural hazards intersect with human security challenges such as tribal conflict, election violence, piracy, cyber intrusions, and cross-border incursions. This convergence increases the likelihood of cascading crises where one event triggers a chain of security, humanitarian, and governance failures. Therefore, PNG's contingency planning must adopt an all-hazards approach that integrates intelligence, logistics, communications, and civil-Military cooperation.

The Disaster Management Act and the National Disaster Risk Reduction Framework (2017–2030) provide baseline policy guidance, outlining responsibilities for the National Disaster Centre (NDC), provincial disaster committees, and security agencies. However, implementation challenges remain due to limited resources, inconsistent political support, and varying levels of provincial capability. As demonstrated by the 2018 Highlands earthquake and subsequent humanitarian bottlenecks, PNG's response capacity is often hindered by slow deployment, limited aircraft availability, inadequate communication systems, and insufficient coordination among agencies.

To strengthen crisis readiness, PNG requires a more structured and intelligence-driven planning cycle. This includes regular risk assessments that incorporate political, social, economic, and climatic indicators. Intelligence from NIO, MILITARY Military Intelligence, RPNGC, provincial authorities, and community networks must be fused to produce early-warning products and predictive models. These assessments can help identify potential flashpoints such as rising election tensions, foreign illicit activity, tribal mobilization, or signs of impending natural hazards.

A robust crisis response also relies on clear command and control structures. PNG's experience shows that during emergencies, confusion over authority between provincial governments, police

commands, and national agencies can delay action. Codifying emergency command frameworks—particularly for responses involving MILITARY—helps eliminate ambiguity and ensures rapid mobilization. Liaison officers, pre-designated incident commanders, and unified operational doctrines contribute to efficient decision-making.

Logistics planning is another critical pillar. PNG's terrain and limited road networks mean aircraft, maritime assets, and remote-area teams must be pre-positioned. Stockpiles of emergency supplies, medical kits, communication equipment, and portable infrastructure should be strategically located across the country. Partnerships with the private sector—especially aviation, telecommunications, and extractive industry operators—can expand national capacity during high-impact events.

Communication resilience is equally vital. The absence of reliable networks during crises disrupts situational awareness and operational control. PNG's contingency plans must prioritize redundant systems—HF radio, satellite communication, encrypted mobile networks, and interoperable devices shared across agencies. Maintaining these systems is essential to avoiding operational paralysis during major disasters or cyberattacks.

Finally, contingency planning must include public messaging strategies to prevent panic, misinformation, and social unrest. Transparent updates, community engagement, and culturally adapted communication help sustain public trust and ensure cooperation with authorities.

In summary, stronger contingency planning will enable PNG to transform its reactive posture into a proactive, intelligence-driven security model. This shift is essential for building national resilience in an increasingly unpredictable security landscape.

Exercises and Scenario-Based Threat Simulations

Scenario-based simulations are critical tools for strengthening national preparedness, identifying operational weaknesses, and building interagency cohesion within Papua New Guinea's security architecture. For a country that faces both traditional and non-traditional threats, simulation exercises offer a structured method to test planning assumptions, evaluate decision-making processes, and measure the readiness of agencies under realistic conditions.

PNG's geography, resource limitations, and evolving threat environment make simulations even more vital. Unlike large militaries with abundant assets, MILITARY, NIO, and RPNGC must rely heavily on planning accuracy, rapid coordination, and improvisation. Simulations help compensate for resource constraints by improving human capability, strengthening networks, and creating shared operational understanding across agencies.

Several types of exercises are applicable to PNG:

Tabletop Exercises (TTX):

These are discussion-based workshops where senior leaders test decision-making against hypothetical but realistic scenarios. They allow agencies to examine policies, identify gaps in legal frameworks, and refine command structures. Tabletop exercises are particularly useful for testing election security plans, cyber incident responses, and diplomatic-security coordination during foreign interference events.

Field Training Exercises (FTX):

These test the physical deployment of personnel and assets in real environments. MILITARY uses FTXs to rehearse border patrols, amphibious landings, disaster response, and urban operations. Joint FTXs with RPNGC improve coordination during riots, high-risk arrests, or counter-insurgency situations. Such exercises build interoperability and reduce friction during real operations.

Multi-agency Crisis Simulations:

These are essential for complex events such as large-scale tribal warfare, mass-casualty disasters, airport security incidents, or foreign-linked criminal activity. They bring together intelligence, logistics, health, transport, and local authorities. These exercises expose communication failures, highlight unclear authorities, and test how quickly agencies can generate a unified threat picture.

Cybersecurity Simulations:

With PNG's increasing reliance on digital systems, cyber simulations test resilience against hacking, ransomware, foreign digital espionage, and critical infrastructure breaches. They also strengthen collaboration between the Cybercrime Unit, NIO, Department of ICT, and external partners.

Red-Team Exercises:

Global intelligence agencies use "red teams" to emulate adversary behaviour, testing the ability of security forces to detect hostile intent and respond effectively. PNG can adapt scaled versions, such as simulated foreign interference attempts, intelligence leaks, or organized crime infiltration scenarios.

These exercises produce several benefits:

- Improved interagency communication
- Stronger analytical capability and threat anticipation
- Identification of training gaps and logistical weaknesses
- Enhanced public safety during major events
- Increased trust and interoperability between institutions

A major advantage of scenario-based simulations is their ability to reveal hidden vulnerabilities that would otherwise remain untested. For example, an election security simulation may reveal that police reinforcement cannot arrive on time due to roadblocks or lack of airlift. A cyber simulation may expose reliance on unsecured networks. A border incident simulation may show that intelligence was available but never shared due to bureaucratic delays.

For PNG, simulations must be iterative, culturally informed, and realistically constrained. Scenarios should incorporate tribal alliances, local political dynamics, terrain challenges, and historical patterns of conflict. Community participation increases realism, especially in simulations involving displacement, humanitarian crises, or civil unrest.

Finally, all exercises must be followed by After Action Reviews (AARs)—structured evaluations that identify strengths, weaknesses, and required reforms. Without AARs, simulations risk becoming symbolic events with no operational impact.

By institutionalizing scenario-based training as a core pillar of national security preparedness, PNG can significantly enhance its resilience, decision-making agility, and early-warning capability. These exercises cultivate a proactive security culture—one in which agencies anticipate threats rather than react to them.

Chapter 7: Countermeasures and Strategic Defense

Mitigation Strategies for Identified Vulnerabilities

Mitigating national security vulnerabilities requires a layered, adaptive and intelligence-driven approach that addresses Papua New Guinea's (PNG) unique geopolitical, socio-cultural and technological landscape. PNG's vulnerabilities—ranging from porous maritime borders, weak digital infrastructure, limited policing capacity, socio-economic pressures, foreign influence, and organized crime—are amplified by the country's diverse terrain and decentralized governance systems. Effective mitigation begins with understanding that threats in PNG rarely operate in isolation; rather, they are multidimensional, overlapping across political, social, technological and transnational spheres. As such, security planners must integrate whole-of-government and whole-of-society mechanisms.

One priority mitigation strategy is strengthening border management through integrated surveillance networks. PNG's maritime borders remain highly susceptible to illegal fishing, arms trafficking, narcotics movement, and unauthorized foreign actors. Mitigation therefore requires a fusion of patrol capacity, satellite maritime domain awareness (MDA), inter-agency intelligence fusion and community-based reporting. Research shows that small states with vast maritime zones, such as Fiji and Solomon Islands, have successfully adopted hybrid models combining local knowledge with technology-based monitoring (Powles, 2022). PNG can draw from these regional parallels to build a more responsive, sustainable framework.

Another key mitigation strategy is institutional strengthening**,** especially within the PNG Defence Force, Royal Papua New Guinea Constabulary (RPNGC), National Intelligence Organisation (NIO) and provincial disaster/security committees. Institutional weaknesses—lack of resourcing, outdated doctrines, slow procurement systems, and corruption vulnerabilities—significantly increase the risk of foreign penetration or exploitation by transnational criminal organizations. Mitigation, therefore, must include doctrine reform, leadership development, transparent procurement, and digitized record systems to prevent unauthorized data access.

Further mitigation must focus on the **protection of critical infrastructure**, including ICT networks, energy systems (PNG Power assets), ports, cellular networks, and financial systems. As hybrid warfare globally blends cyberattacks with influence operations (Rid, 2020), PNG must transition toward cyber

hygiene policies that mandate secure data governance across government agencies. Business-email-compromise attacks in PNG have increased (CERT-PNG, 2023), demonstrating the need for endpoint protection, encryption standards, and digital forensics capabilities.

Mitigation also extends to political resilience**,** especially safeguarding national decision-making from coercion, bribery and foreign influence. The growth of external actors—state and non-state—seeking strategic footholds in PNG necessitates strong oversight, security vetting of political aides, and continuous counter-influence monitoring. Strengthening the Integrity of Political Parties and Candidates Commission provides an institutional point for mitigating political manipulation or covert financing.

Finally, mitigation strategies must empower local communities**,** who are often the first observers of suspicious activity. In rural border regions, community intelligence networks can detect foreign vessels, unusual land purchases, illegal logging operations, or movements of organized crime groups. Community-based threat reporting, supported by mobile platforms and district-level security liaison officers, significantly improves early warning.
Through these layered strategies, PNG can progressively reduce its vulnerability exposure while enhancing national resilience.

Counter-Intelligence Measures: Detection and Disruption

Effective counter-intelligence (CI) is the backbone of national security for any state facing external interference or internal subversion. CI in the PNG context must address a complex blend of actors—foreign intelligence services, organized crime syndicates, corrupt insiders, extremist networks, and opportunistic political actors. Detection and disruption require systematic intelligence capabilities that are proactive, not reactive.

A foundational CI measure is **insider-threat detection**, recognizing that hostile actors often exploit institutional weaknesses through internal collaborators. Global studies show that insider leaks constitute one of the highest national security risks (Rosenbach & Peritz, 2009). PNG's public service structure, characterized by high turnover, inconsistent record-keeping, and political appointments, heightens susceptibility. Implementing personnel vetting, periodic background checks, lifestyle audits and confidential reporting channels can significantly reduce insider manipulation.

CI detection capacity must also expand into the digital domain**,** where hostile intelligence actors increasingly operate. Cyber espionage campaigns targeting Pacific governments have increased in the last decade (Australian Cyber Security Centre, 2022). PNG requires digital forensics laboratories, malware analysis teams, and cyber-intelligence officers trained to detect spear-phishing, credential harvesting, and covert network infiltration. These capacities must be integrated into the National Cyber Security Centre and coordinated with the NIO.

Another CI priority is pattern-of-life analysis**,** where intelligence officers observe and analyze behavioural deviations indicating foreign recruitment, coercion, or undue influence. Suspicious foreign funding, unexplained wealth, frequent cross-border travel, high-level foreign interactions, and sudden changes in communication behaviour are all indicators requiring investigation. Training CI officers in structured analytic techniques enhances accuracy and reduces cognitive bias (Heuer, 1999).

Disruption strategies involve neutralizing hostile operations before they materialize into strategic threats. These include asset freezing for individuals linked to foreign intelligence operations, surveillance of suspicious land acquisitions, disruption of organized crime networks supplying information to foreign actors, and coordinated law enforcement raids. Inter-agency taskforces—NIO, MILITARY Military Intelligence, RPNGC CID, and Immigration—are essential in integrating detection-to-disruption processes.

CI disruption also includes information shielding**,** ensuring sensitive government data is protected from unauthorized access. Establishing secure communication systems for Cabinet, Defence and Intelligence agencies, along with encrypted document management, can prevent foreign interception.

Lastly, CI measures must include strategic deception**,** where security agencies deliberately mislead hostile actors to expose their networks. Controlled leaks, monitored communications, and false flag channels can be used to identify penetrations. This method is used widely across intelligence services globally and can be adapted to PNG's scale and resource environment.
Counter-intelligence success is measured not by what becomes public, but by what threats are quietly neutralized before they grow roots.

Technology-Enhanced Defense Systems

Modern defense strategy globally—and increasingly in the Pacific—prioritizes technological superiority as a force multiplier for states with limited manpower, such as PNG. Technology-enhanced defense systems provide early warning, surveillance, precision, and resilience against hybrid threats.

One critical capability is **integrated surveillance architecture**, combining drones, maritime radars, satellite feeds, ground sensors and mobile patrol units. For PNG's vast Exclusive Economic Zone (EEZ), unmanned aerial vehicles (UAVs) provide cost-effective monitoring of illegal fishing, unauthorized foreign vessels and environmental violations. Regional neighbours like Fiji and Vanuatu already utilize UAVs for similar tasks (Dobell, 2021). PNG's defense modernization plan should include both tactical drones for border patrol and strategic long-endurance systems.

Another essential technology enhancement is secure communications networks for the police and the Military as well as national intelligence agencies. Encryption, quantum-resistant systems, and secure radio networks reduce interception risks. A dedicated national defense intranet allows classified communication insulated from public networks.

Developing cyber defence systems is equally crucial. PNG must build a defensive cybersecurity posture capable of threat hunting, intrusion detection, encryption, and incident response. Cyber defense is no longer separate from physical defence; rather, it protects national infrastructure, financial systems, police networks and even Military operations. Nations without cyber capacity become vulnerable to ransomware, espionage, data theft and foreign influence operations (Clarke & Knake, 2019).

Technology-enhanced defence also includes GIS-based threat mapping**,** AI-supported risk prediction**,** and biometric border control**.** For PNG's airports and ports, biometrics significantly reduce human error and corruption in immigration processes. Smart cameras, license-plate recognition systems and automated watchlist alerts also support CI and law enforcement.

Furthermore, public-private partnerships are increasingly vital. Telecom companies, banks, aviation authorities and energy utilities all control critical nodes that hostile actors may target. Joint threat intelligence sharing and cybersecurity exercises can strengthen national resilience.

For the MILITARY, modernization must balance international partnerships with sovereignty. Collaborations with Australia, the U.S., Japan and Indonesia can bring training and equipment, but PNG must maintain control over data sovereignty and operational independence. Technology enhances defence only when integrated into a coherent national strategy, grounded in PNG's context, terrain, and threat realities.

Building Resilience: Training, Awareness and Community Engagement

Resilience is the foundation of a secure nation. It is not merely the ability to absorb shocks, but to anticipate, adapt and recover from threats. In PNG, resilience-building requires investment in people—soldiers, police, public servants, village leaders, youth, civil society, and frontline communities.

A first pillar of resilience is professional training for security personnel. MILITARY, RPNGC, NIO and provincial security teams must undergo continuous capacity-building in intelligence analytics, cyber awareness, interrogation, surveillance detection, crisis communication and incident response. As global security challenges evolve, static training quickly becomes obsolete. Capacity-building partnerships with regional allies can accelerate PNG's transformation into an intelligence-competent state.

Awareness-building extends beyond security institutions. National security awareness programs for the public—including schools, universities, churches and community groups—help citizens recognize suspicious behaviour, online scams, misinformation campaigns and foreign influence attempts. Public awareness is a critical early-warning system, especially in rural areas where state presence is limited.
Community engagement is the heart of PNG's resilience model. Local communities are the eyes and ears of the nation. Village court officials, ward councilors, women's groups, youth groups and church leaders play crucial roles in identifying emerging threats—illegal logging, unexplained foreign visitors, human trafficking, firearm movement or political manipulation. Strengthening community-level reporting channels, including SMS-based reporting and district security liaison officers, creates a bottom-up intelligence pipeline.

Another crucial component is **psychosocial resilience**, especially in communities exposed to violence, disasters, or foreign exploitation. Resilient populations are harder to manipulate. Trauma-informed

awareness training can help villages resist recruitment by criminal syndicates or exploitation by foreign actors posing as investors.

Resilience-building also requires inclusive participation**,** ensuring women, youth and marginalized groups are represented in security dialogues. Women's groups in PNG have historically been central to peace-building efforts (McKenna, 2019), and their involvement strengthens community security networks.

Finally, resilience depends on the trust between citizens and state institutions. Corruption, abuse of power, or slow response times weaken public willingness to cooperate. Improving professionalism, transparency, and discipline—especially within security forces—creates a virtuous cycle of trust and cooperation.

A resilient PNG is one where every citizen, from the Highlands to the Islands, understands their role in safeguarding the nation.

Chapter 8- Threat Assessment in Action

Real-Time Threat Monitoring and Intelligence Cycle

Real-time threat monitoring is the operational engine of national security. In Papua New Guinea (PNG), where threats evolve rapidly—from tribal conflict escalation to foreign interference, political destabilization, organized crime, cyber intrusions and economic coercion—the ability to observe, analyze and act in real time becomes essential. Effective threat monitoring requires a synchronized intelligence cycle: direction, collection, processing, analysis, dissemination, and feedback. This cycle turns raw observations into actionable intelligence that guides national decision-making at both the strategic and tactical levels.

The Intelligence cycle begins with direction, where leaders articulate priority intelligence requirements (PIRs). For PNG, PIRs might include tracking transnational criminal syndicates, monitoring illegal maritime incursions, identifying foreign influence operations, or detecting potential unrest in Highlands provinces. Direction ensures agencies such as the National Intelligence Organisation (NIO), PNG Defence Force (MILITARY) Intelligence Wing, and Royal Papua New Guinea Constabulary (RPNGC) focus resources on what matters most.

Collection involves gathering raw data: human intelligence from communities, signals intelligence (SIGINT), cyber intelligence from network monitoring, aerial or satellite surveillance, social media analytics, and law-enforcement reports. PNG's diverse geography—mountains, islands and maritime areas—requires blended collection strategies that integrate village-level reporting with technology-enhanced systems such as drones, maritime domain awareness tools, and cyber incident logs.

Once collected, information moves to processing and exploitation, where it is filtered, authenticated, decrypted, translated or organized into structured formats. In PNG, processing often requires validating community reports, separating rumours from credible threats—an essential task given the spread of misinformation and political gossip during periods of unrest.

Analysis is the heart of threat assessment. Analysts interpret data, identify correlations, assess likelihoods, and generate threat forecasts. Methodologies such as link analysis, pattern-of-life tracking, probability assessments, and structured analytic techniques reduce cognitive bias and ensure

objectivity (Heuer, 1999). For national-level monitoring, analytical fusion cells combining MILITARY, NIO, RPNGC, and Customs enhance accuracy by integrating different perspectives.

Dissemination ensures intelligence reaches operators and policymakers quickly. A threat warning delivered too late is equivalent to no warning at all. Secure communication systems, classified briefings, and rapid situational reports (SITREPs) are essential in PNG, especially during crisis responses or border violations.

The final stage—feedback—allows operators and decision-makers to adjust PIRs, correct intelligence gaps, and refine monitoring tools. Without feedback, agencies operate blindly. With feedback, the intelligence cycle becomes adaptive, learning from each operation and improving future monitoring accuracy.

Through this dynamic cycle, PNG can detect emerging threats before they escalate, enabling proactive and coordinated national security responses.

Profiling High-Risk Entities

Profiling high-risk entities is a critical component of threat assessment. It involves systematically identifying individuals, groups, organizations or states capable of causing harm to national security interests. In PNG, high-risk entities range from transnational crime syndicates and foreign intelligence operatives to radicalized individuals, corrupt political actors, arms smuggling networks, cyber criminals and opportunistic business fronts used for illicit activity.

Effective profiling starts with baseline indicators—characteristics consistently associated with threat behaviour. Globally, entities that pose elevated risk often display financial irregularities, ties to foreign actors, access to weapons, extremist associations, or disproportionate levels of secrecy (Borum, 2015). PNG-specific indicators may include unexplained land purchases by foreign companies, sudden rises in wealth among local power brokers, suspicious maritime activities around the Bismarck Sea, and political financing linked to external interests.

Profiling requires a holistic approach that draws from multiple intelligence disciplines. Human intelligence from communities, security officers, and village leaders helps identify unusual behaviour

or foreign presence in remote areas. Cyber intelligence flags suspicious online transactions, encrypted communications, or foreign manipulation on social media. Financial intelligence identifies money-laundering patterns that often precede corruption or organized crime penetration. Geospatial intelligence highlights logistical patterns—such as repeated vessel movements or remote airstrip usage—associated with smuggling operations.

PNG's intelligence agencies must also consider psychological and behavioural profiling. This includes identifying grievances, ideological motivations, personal instability, or susceptibility to foreign recruitment. Behavioural indicators such as secrecy, isolation, sudden travel patterns or drastic lifestyle changes can signal recruitment by external actors. International frameworks like the FBI's behavioural threat assessment model (Meloy & Hoffman, 2021) can be adapted to PNG's context.

A critical component of profiling is cultural intelligence. PNG is one of the most culturally diverse nations on earth, with over 800 languages and localized power structures. Profiling cannot rely solely on Western models; it must integrate clan dynamics, tribal alliances, local hierarchies, and customary practices. Understanding these dynamics enables analysts to differentiate between legitimate community leadership actions and suspicious behaviour that may be exploited by foreign entities or criminal groups.

Finally, profiling requires continuous verification. Entities initially assessed as low-risk can evolve into threats, while high-risk entities sometimes neutralize through reforms, monitoring or deterrence. A living, evolving threat profile system ensures PNG remains one step ahead of those who seek to exploit national vulnerabilities.

Decision-Making Under Uncertainty

National security decision-making almost always occurs under uncertainty. Intelligence rarely offers perfect clarity; instead, leaders must make choices with incomplete, conflicting or ambiguous information. For PNG—facing volatile political dynamics, foreign influence, tribal instability, rapid urban crime shifts, and cyber vulnerabilities—decisions must balance urgency with caution.

Decision-making under uncertainty requires embracing probability, scenario planning, and structured judgment. Intelligence assessments should present confidence levels rather than rigid conclusions. For

example, analysts may state there is a “high likelihood” of a foreign fishing vessel conducting illegal surveillance operations, or a “moderate probability” of political unrest escalating in Hela Province. These probabilistic assessments help decision-makers weigh risks.

Cognitive biases pose major challenges. Confirmation bias, groupthink, anchoring and optimism bias often distort decisions during crises. Training in structured analytic techniques—such as Analysis of Competing Hypotheses (ACH), red-teaming, and scenario stress-testing—helps reduce these flaws (Pherson & Pherson, 2019). MILITARY and NIO officers, especially those in intelligence, benefit greatly from bias-aware leadership training.

Decision-making also depends on time pressure. Security threats may require immediate action, leaving little time to gather additional intelligence. In these cases, leaders must apply the “satisficing” principle—acting on the best available information that meets minimum thresholds of reliability (Kahneman, 2011). Waiting for perfect clarity can cost lives or allow hostile actors to exploit the delay.

PNG’s decision-making must also integrate local insights. Community leaders, district administrators, women’s groups and provincial security committees often spot early signals long before formal intelligence systems detect them. Incorporating local knowledge reduces uncertainty and provides cultural context to ambiguous intelligence.

Finally, decision-making under uncertainty demands accountability. Decisions must be documented, data-driven and subject to review. Lessons learned—from both successes and failures—create institutional memory and enhance future choices. In fast-changing threat environments, decision-making becomes not a single event but a continuous learning process.

Case Studies: Prevented Attacks and Lessons Learned

Case studies allow security agencies to learn from real incidents—examining what worked, what failed and what can be improved. While many operations in PNG remain classified, several generic case models illustrate how threat assessments prevent attacks and strengthen national security.

One illustrative case involves disrupting an organized crime smuggling operation in PNG’s maritime zone. Intelligence from coastal communities reported unfamiliar vessels docking at night. Maritime

domain awareness systems detected irregular movement patterns consistent with transnational drug trade routes used across the Pacific. Collaboration between NIO, the Military's Maritime Element and RPNGC enabled coordinated surveillance and interception. The lesson learned: community reporting, when integrated with technology-enhanced monitoring, creates early-warning capability far stronger than either component alone.

Another relevant case model involves a foreign influence operation targeting senior officials. Analysts noted unusual financial activity, repeated foreign contacts, and attempts to influence policy discussions. After cross-checking financial intelligence, interviewing informants, and analyzing communication patterns, CI officers intervened before the network could establish deeper political leverage. The key lesson: sustained monitoring of political influence indicators reduces the risk of covert foreign penetration.

A third case model relates to cyber intrusion attempts against a PNG government department. A spear-phishing campaign targeted senior staff, attempting to extract login credentials. Cyber intelligence teams identified indicators of compromise and isolated affected systems. Rapid response prevented data exfiltration. Lessons include the importance of cyber hygiene training and rapid incident reporting.

These case studies demonstrate that threat prevention relies heavily on integrated intelligence systems, community cooperation, rapid decision-making, inter-agency collaboration and continual adaptation. Each prevented attack reinforces the same principle: proactive intelligence saves lives, protects national sovereignty and strengthens PNG's long-term stability.

Chapter 9: Cyber Frontiers and Emerging Threats

Digital Espionage Tactics

Digital espionage has become the dominant intelligence collection method of the 21st century, surpassing traditional human intelligence in scale, speed, and strategic reach. Unlike conventional spying, which relies on physical infiltration and interpersonal recruitment, cyber espionage operates through networks, devices, and data infrastructures that underpin modern governance, security, and commerce (Kello, 2017; Rid, 2020). States, non-state actors, criminal syndicates, and hybrid threat groups now conduct intelligence collection remotely, persistently, and often invisibly.

At its core, digital espionage involves unauthorized access to information systems for the purpose of intelligence extraction. Common tactics include phishing campaigns, malware implantation, zero-day exploits, supply-chain compromise, credential harvesting, and remote access trojans (RATs) (Clarke & Knake, 2019). These methods allow attackers to map networks, monitor communications, extract classified documents, and manipulate systems without immediate detection. Advanced Persistent Threats (APTs) represent the most dangerous form of digital espionage due to their patience, stealth, and strategic coordination.

Phishing remains one of the most effective entry points for cyber espionage. Through carefully crafted emails, messages, or fake login portals, attackers exploit human trust rather than technical weakness. Once credentials are stolen, attackers gain legitimate access, making detection difficult (Mitnick & Simon, 2011). In government and security institutions, a single compromised account can cascade into total network exposure.

Malware-based espionage enables long-term surveillance. Spyware embedded in compromised devices can activate microphones, cameras, keystroke logging, GPS tracking, and file exfiltration. This allows adversaries to build behavioral profiles of officials, track operational movements, and identify pressure points for coercion or manipulation (Kello, 2017). In fragile states, where cybersecurity hygiene is uneven, malware infections may persist undetected for years.

Supply-chain attacks represent a rising frontier of digital espionage. Rather than attacking a government agency directly, adversaries compromise software updates, telecommunications vendors, or IT service providers and then use these trusted channels to gain access to multiple targets

simultaneously (Clarke & Knake, 2019). This method transforms civilian infrastructure into silent intelligence collection platforms.

For Papua New Guinea, digital espionage risk is amplified by rapid mobile phone adoption, expanding cloud services, foreign-built telecommunications infrastructure, and limited indigenous cybersecurity capability. National institutions increasingly depend on digital platforms for payroll, taxation, border management, elections, and security coordination. Each system represents a high-value intelligence target (Dinnen & Allen, 2016; PNG ICT Authority, 2020).

The strategic danger of digital espionage lies not only in data theft but in decision-shaping. When adversaries possess internal communications, negotiation positions, personnel vulnerabilities, and classified threat assessments, they gain the ability to preempt, manipulate, and neutralize national policy long before overt confrontation occurs (Rid, 2020). Power is shifted silently from the state to the intruder.

Effective defense against digital espionage requires more than software solutions. It demands cyber doctrine, trained cyber personnel, red-team testing, threat intelligence fusion, and continual security culture reinforcement across all levels of government and security forces (Gill & Phythian, 2018). Cyber defense is now inseparable from national defense.

AI and Automation in Threat Detection

Artificial intelligence and automation have fundamentally transformed the speed, scale, and accuracy of modern threat detection. Traditional security systems relied on human analysts reviewing alerts, logs, and reports after incidents had already occurred. In contrast, AI-driven systems operate continuously, analyzing massive volumes of data in real time to identify anomalies, behavioral patterns, and predictive risk indicators before damage escalates (Russell & Norvig, 2021; Kello, 2017). Machine learning algorithms now detect cyber intrusions by recognizing deviations from normal network behavior rather than relying solely on known attack signatures. This allows security systems to identify previously unseen attack methods, including zero-day exploits and custom malware (Goodfellow et al., 2016). Behavioral analytics further enhance detection by monitoring user activity patterns and flagging insider threats, compromised accounts, and coercion-related anomalies.

Automation also enables rapid defensive response. Once a hostile activity is detected, systems can isolate infected endpoints, revoke credentials, reroute traffic, and preserve forensic evidence within milliseconds. This compresses the attacker's operational window and significantly reduces damage potential (Clarke & Knake, 2019). In national security environments, automation increasingly determines whether breaches become contained incidents or strategic failures.

AI is also transforming physical security intelligence. Facial recognition, gait analysis, drone surveillance, biometric border screening, and predictive policing tools allow governments to monitor movement patterns, identify suspects, and map threat networks at unprecedented scale (Russell & Norvig, 2021). However, these capabilities introduce major ethical, legal, and civil liberty challenges when improperly governed.

In the Asia-Pacific region, states are racing to adopt AI-enabled security systems for cyber defense, counterterrorism, maritime surveillance, financial crime detection, and border protection. The asymmetry is dangerous: institutions without AI capability become blind in an environment where adversaries operate at machine speed (Kello, 2017).

For Papua New Guinea, the promise of AI in threat detection is substantial but constrained by infrastructure gaps, data scarcity, cybersecurity maturity, and skills shortages. Automated systems can assist in detecting fraud, cyber intrusion, election interference, transnational crime financing, and illegal border movement. However, without strong data governance and trained analysts, AI risks becoming either ineffective or externally dependent (Gelu, 2013; PNG National Research Institute, 2019).

Automation also reshapes intelligence labor itself. Analysts increasingly become supervisors of algorithmic outputs rather than sole decision-makers. This introduces the risk of automation bias, where human judgment defers too readily to machine recommendations. In high-stakes security environments, blind trust in algorithms can produce catastrophic miscalculations (Russell & Norvig, 2021).

AI-driven detection systems must therefore be embedded within structured intelligence training, legal oversight, and ethical governance. Technology without doctrine becomes vulnerability. For PNG, future cyber security strength will rest not just on acquiring AI systems, but on developing sovereign control over how those systems are trained, deployed, and regulated.

Social Media and Psychological Operations

Social media platforms have become the primary battlespace for modern psychological operations (PSYOPS). Unlike traditional propaganda delivered through radio, print, or television, social media enables direct, personalized, algorithm-driven influence over emotions, beliefs, and behavior at population scale (Wardle & Derakhshan, 2017; Rid, 2020). Influence now operates through likes, shares, outrage cycles, trending narratives, and viral identity reinforcement.

Psychological operations in the digital age are built on three core functions: perception shaping, emotional manipulation, and behavioral activation. Through targeted messaging, coordinated inauthentic accounts, influencer cultivation, bot amplification, and disinformation cascades, threat actors engineer social reality rather than merely commenting on it (Wardle & Derakhshan, 2017).

Fear, grievance, humiliation, pride, and outrage serve as the primary emotional weapons. Content that evokes strong emotional reaction spreads faster than factual correction. This allows adversaries to destabilize societies by inflaming political polarization, ethnic division, institutional distrust, and social panic (Putnam, 2000; Rid, 2020). Once trust collapses, governance becomes psychologically brittle even if physical infrastructure remains intact.

Social media PSYOPS also exploit identity. Individuals increasingly construct personal meaning through online affiliation. Threat actors insert narratives that associate loyalty, masculinity, patriotism, faith, or resistance with specific political positions. Behavioral compliance then emerges from identity defense rather than rational analysis.

In Papua New Guinea, social media influence operations are especially potent due to strong community networks, youth-dominated online spaces, religious authority flows, and rapid smartphone diffusion without parallel digital literacy expansion. Rumors spread through Facebook groups, WhatsApp chains, TikTok clips, and Messenger broadcasts with limited fact-checking mechanisms (Dinnen, 2001; PNG Media Council, 2020).

Psychological operations also intersect with cybercrime and extortion. Disinformation may be used to justify harassment, coercion, reputational destruction, or electoral intimidation. Once individuals fear social destruction, they become highly susceptible to manipulation.

The national security risk of social media PSYOPS lies in their invisibility. There are no borders, no uniforms, and no clear declaration of hostile intent. Yet public confidence in elections, policing, judiciary, Military, and leadership can be eroded permanently through narrative warfare alone (Rid, 2020).

Defensive response must therefore emphasize psychological resilience, digital literacy, platform governance, fact verification networks, and trusted public communication channels. Cyber PSYOPS are defeated not through censorship alone but through institutional credibility and population-level critical thinking capacity.

Preparing for Future Technological Vulnerabilities

Future technological vulnerabilities will not emerge solely from new inventions but from the interaction between accelerating innovation, uneven governance, and malicious adaptation. Every major technological advance creates parallel opportunity for exploitation (Kello, 2017). The speed of innovation now far exceeds the speed of regulation, training, and institutional adaptation, producing persistent strategic exposure.

Quantum computing represents one of the most disruptive future cyber threats. Once operational at scale, quantum systems will be capable of breaking current encryption standards protecting Military communications, banking systems, diplomatic cables, and classified archives (Clarke & Knake, 2019). States that fail to prepare for post-quantum cryptography may experience retrospective data compromise long after information was assumed secure.

The expansion of the Internet of Things (IoT) introduces vast new attack surfaces. Smart meters, CCTV systems, traffic controls, maritime sensors, medical devices, power grids, and telecommunications infrastructure are increasingly networked but rarely hardened to Military-grade security standards. Compromised IoT networks can be weaponized into botnets, sabotage tools, or surveillance grids (Kello, 2017).

Biometric dependency creates another vulnerability frontier. As states adopt facial recognition, fingerprint authentication, and identity-linked databases, biometric theft becomes far more dangerous

than password compromise. A stolen fingerprint cannot be reset. Once biometric identity is compromised, lifelong impersonation risk emerges (Russell & Norvig, 2021).

For Papua New Guinea, future vulnerability preparedness is constrained by infrastructure gap, skills shortages, procurement dependency, and regulatory lag. Yet these same constraints make proactive planning even more essential. As PNG expands digital government services, smart infrastructure, and mobile financial platforms, cyber resilience must evolve ahead of threat adaptation (PNG ICT Authority, 2020; NRI, 2019).

Institutionally, preparedness requires forward threat modeling rather than reactive breach response. National security systems must integrate cyber forecasting, technology horizon scanning, red-team simulation, and hybrid threat exercises as routine practice (Gill & Phythian, 2018).

At the societal level, technological resilience depends on education. Cyber hygiene, data ethics, AI literacy, and information verification must become core components of national education and public service training. A digitally powerful society without digital judgment becomes strategically fragile.

The ultimate lesson of emerging cyber vulnerability is clear: technological superiority does not guarantee security. Only disciplined governance, anticipatory intelligence, and societal resilience can prevent the tools of progress from being turned into instruments of national destabilization.

Chapter 10: Insider Threats and Human Factor

Detecting Compromised Personnel

Insider threats are among the most dangerous security risks any organization can face, particularly in intelligence, defence, law enforcement, and sensitive government operations. Unlike external adversaries—who must penetrate physical and digital perimeters—insiders already possess authorized access, institutional knowledge, and operational trust. This makes them uniquely capable of bypassing safeguards and causing significant damage before they are detected.
A compromised insider may intentionally leak classified information, sabotage systems, assist foreign entities, or manipulate internal processes. In Papua New Guinea (PNG), insider threats are amplified by factors such as financial hardship, political pressure, tribal obligations, community expectations, and exposure to foreign influence operations. Detecting compromised personnel therefore requires integrating technology, behavioural monitoring, and organizational vigilance.

Early detection begins with baseline personnel vetting, including background checks, financial assessments, and verification of employment history. PNG's National Intelligence Organisation (NIO), PNG Defence Force and Royal Papua New Guinea Constabulary (RPNGC) increasingly rely on layered vetting processes to identify vulnerabilities before granting access to sensitive information.

Continuous evaluation is equally important. This includes monitoring unusual access patterns, downloading classified documents outside of duty requirements, attempts to access restricted databases, or frequent communication with suspicious individuals or foreign entities. Technology-based systems—such as insider threat detection software and audit logs—provide early-warning indicators of anomalous digital behaviour.

However, detecting compromised personnel cannot rely solely on technology. Human observation remains critical. Colleagues, supervisors, and security officers often detect early behavioural shifts that signal stress, divided loyalty, or manipulation. Creating an organizational culture where personnel feel confident reporting concerns without fear of retaliation is essential to preventing internal compromise.

Behavioral Analysis and Warning Signs

Behavioral analysis plays a central role in identifying insider threats long before they manifest into damaging actions. Research in both psychology and security studies shows that individuals who become compromised often exhibit distinct behavioural indicators. These signs do not always confirm malicious intent, but they provide alerts for deeper assessment.

Common warning signs include sudden changes in work habits, increased secrecy, unexplained wealth, emotional instability, resentment towards leadership, or declining loyalty. In PNG's context, insiders may also display stress linked to tribal obligations, family disputes, gambling debt, romantic manipulation, or pressure from external actors seeking political or economic influence.

Security frameworks such as the Critical Pathway Approach (Shaw & Sellers, 2015) map the psychological journey from personal vulnerability to malicious action. Individuals often move through stages: experiencing a personal grievance, attempting to cope, failing to resolve their issues, and becoming susceptible to external exploitation or self-initiated betrayal.

Behavioural indicators relevant to PNG include:

- Unjustified interest in restricted operations
- Frequent private meetings with foreign officials or business actors
- Attempts to influence decisions in ways inconsistent with organizational priorities
- Attempts to hide personal financial struggles
- Isolation from colleagues
- Increased alcohol use, secrecy, or erratic mood changes
- Complaints about "being undervalued" or "not being recognized"

Security officers in the Military, NIO, and RPNGC benefit from training in behavioural detection, enabling them to distinguish between cultural norms and genuine warning signs. Importantly, behavioural assessments must avoid bias, focusing on patterns rather than isolated actions, and always balancing fairness with national security needs.

Loyalty, Coercion and Blackmail Scenarios

Insiders may become threats due to loyalty conflicts, coercion, manipulation, financial incentives, or blackmail. In PNG, these pressures are often intertwined with local social structures, clan loyalties, and economic vulnerability.

Loyalty conflicts arise when personnel must choose between institutional duty and tribal expectations. Clan leaders or relatives may request information, favors, or operational support. While such requests may appear harmless, they can be exploited by external actors. Foreign businesses or intelligence-linked entities may deliberately target personnel with strong community obligations, manipulating them through social pressure or gifts.

Coercion scenarios involve threats to personal safety, family members, or community standing. Organized crime groups, foreign-backed networks, or corrupt political actors may weaponize fear to force insiders into compliance. Coercion can also occur subtly—through persistent social invitations, financial "assistance," or carefully crafted dependency relationships.

Blackmail scenarios are among the most dangerous. These include compromising photographs, recordings, financial scandals, extramarital relationships, or digital vulnerabilities. PNG personnel are increasingly targeted through social media honey-traps, phishing attacks that steal private information, and staged romantic encounters designed to create leverage. Once blackmail material is obtained, the victim becomes highly exploitable.
Intelligence and defence institutions must prepare personnel to recognize recruitment attempts, manipulation tactics, and exploitation strategies. Regular counterintelligence briefings, anonymous reporting channels, confidential counseling services, and financial literacy training help reduce susceptibility to coercion and blackmail. Strengthening individual resilience directly strengthens national security.

Strengthening Internal Security Culture

A strong internal security culture is the most effective long-term safeguard against insider threats. Culture determines whether security is treated as a daily responsibility or an afterthought. In PNG—

where institutions face resource constraints, rapid political change, and competing social loyalties—building a resilient security culture is vital.

An effective internal security culture includes the following elements:

Clear Leadership Expectations

Senior officers must model integrity and reinforce that national duty overrides clan, political, or financial interests. Leadership behaviour sets the tone for the entire organization.

Continuous Training and Awareness

Personnel should regularly receive updated training on insider threat indicators, cybersecurity, counterintelligence, and responsible reporting. Training must integrate PNG cultural considerations, ensuring relevance and practical application.

Confidential Reporting Channels

Personnel must be able to report suspicious behaviour without fear of retaliation. Anonymous hotlines, whistleblower protections, and confidential discussions with security officers reinforce this system.

Cybersecurity Discipline

With rising digital threats, a culture of cyber hygiene—strong passwords, secure communication practices, and cautious use of social media—is critical across all security agencies.

Regular Audits and Access Controls

Periodic access reviews ensure only those who genuinely require classified information can access it. Segmented access prevents unnecessary exposure to sensitive material.

Community Awareness for Personnel

Families of security officials must understand the risks of foreign manipulation, community pressure, and digital exploitation. A well-informed household contributes to a well-protected officer.

Promoting Psychological Well-being

Many insider threats emerge due to unresolved personal stress. Institutions that provide mental health support, financial counseling, and welfare mechanisms significantly reduce insider threat vulnerability.

Ultimately, internal security culture depends on shared responsibility. When every officer understands that national security begins with personal integrity and vigilance, insider threats lose much of their power. A strong culture transforms every employee into a barrier against infiltration and compromise.

Chapter 11: International Cooperation and Intelligence Sharing

Regional Partnerships: PNG and Pacific Allies

Papua New Guinea's security landscape is increasingly shaped by its regional partnerships across the Pacific. As geopolitical competition intensifies—particularly among major powers such as China, Australia, and the United States—the Pacific Islands have become strategically significant in Military, cyber, and economic domains. PNG's ability to maintain sovereignty and stability depends heavily on effective cooperation with trusted regional allies through information exchange, joint exercises, and coordinated security strategies.

The Pacific Islands Forum (PIF) plays a major role in guiding shared regional security priorities through the Boe Declaration on Regional Security (2018), which emphasises "collective security," "peaceful Pacific societies," and "strengthened information-sharing networks." PNG participates actively in PIF's security working groups that address transnational crime, cyber threats, climate-security risks, and border vulnerabilities.

Australia remains PNG's closest defence and intelligence partner. Through the PNG–Australia Defence Cooperation Program (DCP), Australia provides training, joint maritime patrols, intelligence collaboration, and capacity-building for the PNG Defence Force and the National Intelligence Organisation (NIO). Australia also supports technology transfers, cyber defence strengthening, and maritime domain awareness systems such as the Pacific Maritime Security Program (PMSP) and Guardian-class patrol boats.

The United States has deepened cooperation with PNG through the US–PNG Defence Cooperation Agreement (DCA), Maritime Security Frameworks, and joint training exercises. These partnerships help PNG counter threats such as illegal fishing, foreign intelligence activity, transnational drug trafficking, and grey-zone operations.

PNG also engages with Pacific neighbours such as Fiji, Solomon Islands, and Vanuatu through the Melanesian Spearhead Group (MSG). MSG cooperation includes security dialogues, training, crisis response discussions, and frameworks for intelligence interoperability, particularly through police and defence channels.

These partnerships ensure PNG does not face complex threats alone. By integrating regional intelligence, PNG builds a stronger early-warning system capable of detecting emerging risks at sea, along borders, and in the cyber domain. In the modern security environment, no Pacific nation can operate in isolation—collective vigilance remains the key to resilience.

Legal Frameworks for Cross-Border Intelligence

Intelligence sharing must operate within clear legal boundaries to ensure sovereignty, accountability, and compliance with both domestic and international law. Papua New Guinea's legal system establishes several key instruments governing information exchange, national security activities, and cross-border cooperation.

The National Intelligence Organisation Act 1984 is PNG's primary legislation for intelligence operations. It authorizes the NIO to gather, evaluate, and exchange intelligence relevant to national security. Section 7 of the Act empowers the NIO to collaborate with foreign intelligence agencies when deemed necessary for PNG's security interests, provided such collaboration is authorized by the Minister responsible. This provision forms the legal basis for intelligence-sharing arrangements with Australia, the United States, Pacific allies, and multilateral bodies.

The Defence Act 1974 provides the legal framework for Military participation in joint operations, including collaborative missions with regional Military partners. The Act permits international agreements for training, operations, and shared intelligence during combined tasks such as humanitarian responses, maritime surveillance, and regional stability operations.

Cross-border policing cooperation is grounded in the Extradition Act 2005, the Mutual Assistance in Criminal Matters Act 2005, and the Criminal Code Act 1974 (Provisions on transnational crime, cybercrime, and terrorism financing). These laws allow PNG to request or provide intelligence for criminal investigations, counter-terrorism activities, and tracking transnational syndicates.

At the regional level, PNG is a signatory to the Pacific Transnational Crime Network (PTCN), which facilitates real-time intelligence exchange through Transnational Crime Units (TCUs) operating in multiple Pacific nations. PNG's TCU works closely with INTERPOL, AFP, and regional police forces.

Cyber intelligence sharing is guided by the National Cyber Security Policy (2018) and the work of PNG CERT, which coordinates cross-border cyber incident reporting and digital threat intelligence under global cybersecurity norms.

Together, these legal instruments ensure that PNG's intelligence partnerships operate within lawful boundaries, protecting sovereignty while enabling robust international cooperation.

Case Studies: Collaborative Operations

Collaborative operations demonstrate how intelligence sharing enhances PNG's national security. Although many operations remain confidential, several illustrative regional case models highlight the effectiveness of coordinated action.

One example is Operation Blue Pacific, a joint maritime surveillance initiative involving PNG, Australia, and the United States. Through shared maritime domain awareness data—including satellite monitoring, aerial patrols, and vessel tracking—security agencies intercepted foreign vessels suspected of illegal fishing and potential espionage activities. The operation demonstrated that regional information-sharing networks significantly enhance maritime security across the Bismarck Sea and Coral Sea.

A second example involves a Melanesian Spearhead Group law-enforcement cooperation taskforce, where PNG, Solomon Islands, Vanuatu, and Fiji shared intelligence on a transnational drug trafficking network moving contraband across the Pacific by small craft. Coordinated tracking, financial intelligence, and HUMINT contributed to the seizure of narcotics and the arrest of key operatives. The operation highlighted the value of cultural familiarity and regional trust networks among Melanesian nations.

Cyber threat cooperation provides another instructive model. PNG CERT collaborated with Australian Cyber Security Centre (ACSC) analysts to contain a malware intrusion targeting government email systems. With shared indicators of compromise (IOCs) and rapid intelligence exchange, the breach was isolated before sensitive data was extracted. The case demonstrated that cyber defence requires cross-border situational awareness to counter globally orchestrated internet-based attacks.

In each case, shared intelligence allowed PNG to act decisively against threats that would have been extremely difficult to detect or respond to independently. Regional cooperation magnifies PNG's security capacity and helps ensure national sovereignty in an increasingly contested Indo-Pacific environment.

Risk of Miscommunication and Leakage

While intelligence cooperation strengthens security, it also introduces risks. Miscommunication, misinterpretation, and leakage can compromise operations and damage international trust. These risks are heightened when intelligence is shared quickly across multiple agencies and countries with varying security cultures, technological capacities, and classification standards.

Miscommunication often arises from ambiguity in reporting, differing intelligence assessment methods, or cultural misunderstandings between partner agencies. For example, Pacific reporting styles—which may

emphasize relational context—can differ significantly from Western intelligence formats that prioritize structured, data-heavy assessments. Without standardization, shared intelligence may be misunderstood or operationally misapplied.

Leakage is an even more serious concern. Breaches of classified information—whether deliberate or accidental—can expose sensitive methods, compromise informants, and endanger national security personnel. Leakage may occur through insider threats, unsecured communication systems, cyber vulnerabilities, political interference, or corruption. PNG's cyber infrastructure and physical document security remain areas of continuing vulnerability.

There is also the risk of over-sharing—providing partner nations with more information than legally necessary, potentially exposing PNG to diplomatic consequences. Conversely, under-sharing may cause allies to lose trust or question PNG's reliability.

Mitigating these risks requires robust legal safeguards, secure communication systems, standardized reporting formats, and rigorous training on classification handling. PNG must also strengthen internal counterintelligence measures to ensure that intelligence entrusted by partners is protected from both domestic and foreign exploitation.

Ultimately, intelligence cooperation depends on trust. Any breach—whether miscommunication or leakage—can damage years of diplomatic and operational work. Strong internal safeguards allow PNG to remain a reliable partner in regional and global security networks.

Chapter 12: The Path Forward – Resilience and National Security

The Need for Strategic, Proactive Threat Prevention

In the shifting global and regional security environment, reactive responses to threats — arrests after attacks, damage control following sabotage or infiltration — are no longer sufficient. Modern adversaries employ hybrid tactics, combining cyber-attacks, espionage, sabotage, and influence operations. For a nation such as Papua New Guinea (PNG), with diverse vulnerabilities — geographic fragmentation, fragile infrastructure, complex tribal and regional dynamics, exposure to external economic pressures, and increasing digital dependence — a framework grounded in long-term, multi-domain threat prevention is essential rather than optional.

Such a strategy moves the national security posture from reaction to resilience: anticipating threats, neutralizing vulnerabilities before exploitation, and sustaining stability over decades. It demands a holistic, layered, adaptive architecture that integrates intelligence, infrastructure protection, societal resilience, and inter-agency coordination.

Core Principles of an Effective Long-Term Prevention Strategy

A long-term national threat prevention strategy should be guided by the following core principles:

1. **Intelligence-Led Risk Management** — continuously gather, analyse, and share data across agencies (defence, police, civil, private sector) to identify and assess threats early. This is vital to move beyond episodic threat response into sustained situational awareness. Research from other contexts (e.g., Nigeria's intelligence-led risk management model) shows that institutionalizing collaboration between intelligence and risk-management entities greatly strengthens public safety and national security over time. Jurnal FISIP Universitas Garut

2. **Protection of Critical Infrastructure** — ensure that physical, digital, and societal infrastructure (transport, energy, communications, finance, governance) are secured against sabotage, cyber-attack, and systemic failures. The global rise in infrastructure-targeted threats underscores how vital this principle is.

3. **Cybersecurity & Digital Resilience** — given PNG's increasing digital adoption, protecting digital infrastructure, data, and services is as important as protecting physical borders. PNG's own PNG National Cyber Security Strategy 2024–2030 underscores this need, recognizing cyber threats as core risks to national security, economic stability, and sovereignty.

4. **Whole-of-Society and Community Resilience** — threats often exploit societal vulnerabilities: poverty, ethnic/tribal tension, inequality, social fragmentation, or disenfranchised communities. A long-term strategy must build societal resilience, trust in institutions, and community cohesion, thereby reducing the appeal or operational foothold of non-state actors and subversive influences.

5. **Interagency & International Cooperation** — no security institution can safeguard a nation alone. Coordinated efforts across defence, intelligence, police, civil government, private sector, and — where relevant — international partners, are required. This multiplies capability, share intelligence, and increases deterrence through unity of effort.

6. **Adaptive and Iterative Strategy Design** — threat landscapes evolve: cyber tactics change, geopolitical pressures shift, natural disasters or climate-induced instability arise. The strategy architecture must include mechanisms for regular review, adaptation, feedback loops, and capability upgrades.

Structural Components of a Prevention Strategy

Based on these principles, a robust long-term prevention strategy should include the following structural components:

Establishment of a National Intelligence-Risk Fusion Centre

- A permanent institutional body that fuses intelligence analysis, risk management, disaster-risk reduction, cyber surveillance, and early-warning functions.

- It aggregates data from multiple sources: human intelligence (HUMINT), signals intelligence (SIGINT), open-source intelligence (OSINT), cyber monitoring, community reports, and cross-sector incident data (infrastructure, public safety, finance).
- Its mandate: continuous threat horizon scanning, vulnerability assessment, strategic risk mapping, and issuing periodic national threat assessments.

Such a fusion-center model is extolled in national security literature as one of the most efficient frameworks for maintaining long-term vigilance while avoiding resource wastage or reactive overload.

Critical Infrastructure Protection (CIP) Program

- Inventory and classification: a national register of critical infrastructure (utilities, transport, energy, communications, finance, governance nodes) with prioritized protection status.
- Risk-assessment cycles: periodic audits, vulnerability testing (physical and cyber), stress-testing, and contingency planning.
- Redundancy and resilience: backup systems, fallback protocols, decentralization (where feasible), and community-level contingency planning (particularly for remote provinces and vulnerable regions — important for PNG's dispersed geography).
- Cyber-physical integration: recognizing that threats may be purely digital (cyberattacks) or hybrid (cyber + physical sabotage), and building interlocking defense mechanisms. Citation from modern global CIP frameworks highlights the rising sophistication of threats and the need for generative-AI-aware protection design.

National Cybersecurity Strategy Implementation with Public–Private Engagement

- Institutionalizing the goals of PNG's NCSS 2024–2030: secure government networks, protect citizen data, safeguard private sector critical infrastructure, and foster cyber resilience across society.
- Cyber-hygiene education and awareness campaigns: training government staff, private enterprises, and citizens on basics of cyber hygiene, phishing resistance, data protection, and incident reporting.
- Capacity building: expand digital forensics, incident response, threat-intelligence capability (e.g., training programs like recent digital-forensic training held in 2024 in PNG).

- Information sharing and collaboration: public–private cooperation, shared threat-intelligence platforms, and cross-sector coordination (government, private sector, civil society) to detect, warn, and respond rapidly to cyber threats. This aligns with international best practices of information-sharing environments (ISE).

Community Resilience and Societal Engagement

- Implement community-based early-warning networks: involve local leaders, civil society, religious institutions, NGOs, and community security stakeholders to report suspicions, social grievances, or early signs of radicalization or external manipulation.
- Social development and inclusion: address socio-economic vulnerabilities (poverty, inequality, unemployment, marginalization) to reduce the appeal of criminal or subversive actors. In a fragile context like PNG — where regional disparities, tribal tensions, and resource pressures exist — social stability becomes a security asset.
- Public-awareness and civic education: build national consciousness about internal threats (espionage, infiltration, corruption, sabotage), counter-intelligence awareness, civic responsibility, and resilience culture — making citizens active participants in national security, rather than passive observers.

Institutional & Legislative Frameworks; Oversight and Policy Governance

- Draft and enact a comprehensive Internal Security White Paper or legislation that defines national security architecture, roles and responsibilities, inter-agency coordination mechanisms, oversight, accountability, and transparency — ensuring institutional longevity and legitimacy. PNG has already signaled intent to create such a White Paper
- Periodic strategy review boards: establish a National Security Capability Review Board (or equivalent) to audit, assess, and evolve security strategies every 3–5 years, adapting to new threats, technology shifts, and emerging vulnerabilities.
- Integration with disaster-risk reduction and emergency preparedness frameworks — because in a country like PNG, natural disasters (climate-induced events, earthquakes, floods) often intersect with security vulnerabilities. For example, the national disaster-risk framework 2017–2030 provides a foundation for long-term hazard mitigation strategies.

Anticipating Challenges and Countermeasures

A long-term prevention strategy must also anticipate internal and external challenges: resource limitations, political will fluctuations, corruption risks, uneven capacity distribution across regions, and evolving threat sophistication (cyber-actors, non-state actors, foreign espionage). To mitigate these risks:

- Prioritize capacity-building and training across all sectors — intelligence, cyber, civil administration, local communities.
- Maintain transparency and oversight to prevent abuse of security apparatus — balancing secrecy and civil rights to preserve legitimacy.
- Cherish adaptability and continuous learning — embed war-gaming, scenario planning, red-teaming, and after-action reviews into doctrine and training.
- Promote regional and international cooperation — partner with friendly nations, regional bodies, and global institutions to share intelligence, resources, and best practices.

Implementation Roadmap (Short-, Medium-, and Long-Term Phases)

Short-term (1–2 years):

- Establish the national intelligence-risk fusion center
- Begin infrastructure audit & critical-infrastructure register
- Launch nationwide cyber-hygiene education and capacity building
- Draft and adopt the Internal Security White Paper / policy framework
-

Medium-term (3–5 years):

- Implement infrastructure protection upgrades, redundancy systems, and secure backups
- Institutionalize regular risk assessments, audits, and threat horizon scanning
- Expand community engagement networks, civic education, and social-resilience programs
- Strengthen inter-agency and public-private collaboration, information-sharing platforms, and international intelligence cooperation

Long-term (5–15+ years):

- Maintain adaptive security doctrine with periodic review boards
- Sustain capacity building, training, and institutional memory preservation
- Monitor evolving threat landscape (cyber, climate, geopolitics) and update strategies accordingly
- Embed security resilience in national development planning — making stability and safeguarding an ongoing, integrated component of national growth

Why This Strategy Matters for Papua New Guinea

For PNG, adopting such a long-term, multi-layered strategy is not just academic — it is essential for survival and sovereignty. As described in external analyses of PNG's fragility, the country's weaknesses (economic dependence, social divisions, diverse geography, vulnerability to external economic and political pressures) make it especially exposed to hybrid threats, external interference, and internal destabilization.

Implementing a prevention-oriented strategy means transforming threats into manageable risks — preserving national cohesion, protecting critical infrastructures, safeguarding digital and physical sovereignty, and empowering citizens as part of a collective security culture.

Strengthening Institutions and Intelligence Capacity

Strengthening institutions and intelligence capacity is a foundational pillar of long-term threat prevention. In an era where security threats are increasingly complex, transnational, and technologically enabled, weak institutions create strategic gaps that hostile actors exploit. Strong institutions provide continuity, legitimacy, accountability, and operational effectiveness across intelligence, defence, law enforcement, border control, cyber security, and judicial systems. For Papua New Guinea and similar developing security environments, institutional resilience is not merely administrative reform; it is a national survival imperative.

Institutional strength begins with governance. Intelligence and security agencies require clear legal mandates, transparent oversight mechanisms, and professional standards that align with democratic accountability. Without these, institutions risk politicization, corruption, and erosion of public trust,

all of which degrade intelligence effectiveness (Bruneau & Boraz, 2007; Gill & Phythian, 2018). Public confidence is particularly critical in intelligence work because community cooperation is often the primary source of early warning. When citizens view institutions as legitimate and professional, they are more likely to report suspicious activity and support counter-threat operations.

Capacity building must extend beyond personnel numbers to include doctrine, training, leadership development, and technological modernization. Intelligence capacity is not defined solely by collection ability but by the full intelligence cycle: direction, collection, processing, analysis, dissemination, and feedback. Failures at any stage weaken national threat prevention. Heuer (1999) demonstrated that poor analytical frameworks and cognitive bias often cause greater intelligence failures than lack of data. Strengthening institutions therefore requires structured analytic training, red-teaming practices, and continuous professional education to reduce systemic blind spots.

Human capital remains the most decisive factor in intelligence effectiveness. Long-term prevention requires a sustainable pipeline of trained analysts, field officers, cyber specialists, and operational commanders. This includes standardized induction programs, career progression models, and ethical leadership training. The absence of these systems leads to high attrition, skill drain, and operational inconsistency. In the Pacific context, where regional competition is intensifying, the need for locally trained intelligence professionals who understand cultural, linguistic, and tribal dynamics is particularly critical (Dinnen, Gelu, & Batley, 2013).

Technological capacity is now inseparable from institutional strength. Modern threat prevention requires secure information systems, encrypted communications, surveillance infrastructure, cyber defense platforms, and interoperable databases across agencies. Without these, intelligence remains fragmented and slow. United Nations assessments consistently show that digital intelligence integration significantly improves early-warning systems for terrorism, financial crime, and transnational organized networks (United Nations Office on Drugs and Crime [UNODC], 2021). For PNG, this includes border surveillance technology, maritime domain awareness systems, biometric identity management, and secure intelligence fusion centers.

Equally vital is inter-agency coordination. Intelligence failures often occur not because information is unavailable, but because it is isolated within institutional silos. Police, defence, customs, immigration, financial intelligence units, and cyber authorities must share actionable intelligence in real time. Fusion models adopted in Australia, the United States, and Singapore demonstrate that integrated intelligence

platforms significantly enhance threat detection and disruption (Ratcliffe, 2016). For PNG, where geographic dispersion and resource limitations already strain security coverage, inter-agency fusion is not optional; it is essential.

Institutional resilience also requires strong legislative frameworks. Laws governing surveillance, counter-terrorism, cybercrime, financial intelligence, and border security must evolve in parallel with threat environments. Outdated legislation creates operational blind spots that hostile actors exploit. The Government of Papua New Guinea's National Security Policy and Medium-Term Development Plans recognize institutional reform and intelligence modernization as central to national stability, particularly in response to organized crime, illicit finance, cyber intrusion, and foreign interference (Government of Papua New Guinea, 2013; 2023).

Financial intelligence capacity is another critical pillar of institutional strengthening. Modern threats are sustained by money flows across illicit economies. Strengthening Financial Intelligence Units, banking compliance, asset-tracking capabilities, and international financial cooperation directly weakens criminal and hostile networks. The Asia/Pacific Group on Money Laundering has repeatedly highlighted the vulnerability of Pacific states to money laundering, corruption, and transnational crime and the urgent need for intelligence-driven financial enforcement (APG, 2020).

Leadership integrity is a structural determinant of intelligence credibility. Where leaders lack professional ethics, institutions drift toward patronage, information leaks, and politicized operations. Westoby and Dowden (2010) argue that leadership failure is one of the most consistent predictors of institutional collapse in fragile states. In the PNG context, where clan, political, and economic pressures intersect, intelligence leadership must be deliberately insulated through legal protection, merit-based promotion, and independent oversight.

Institutional strengthening also requires regional and international intelligence partnerships. No modern state prevents threats in isolation. Information-sharing agreements, joint training, maritime surveillance cooperation, cyber threat exchanges, and counter-terrorism task forces extend national detection depth. For PNG, partnerships with Australia, New Zealand, regional Pacific security mechanisms, and multilateral intelligence frameworks significantly enhance early-warning capacity and strategic deterrence (Firth, 2018).

However, institutional reform is not a one-time event; it is a continuous cycle of adaptation. Threat landscapes evolve faster than bureaucratic systems. Long-term prevention therefore demands built-in

mechanisms for institutional learning, audit, scenario testing, and doctrinal evolution. Resilient institutions are not those that resist change, but those that absorb disruption and convert it into improved capability.

Ultimately, intelligence capacity without institutional strength produces fragmented power without strategic direction. Conversely, institutions without intelligence capacity become reactive and blind. Sustainable national security emerges only where both evolve together. For Papua New Guinea, strengthening institutions and intelligence capacity is not only about defending borders and infrastructure; it is about securing national sovereignty, economic stability, social cohesion, and the future leadership of the state.

True security is not built on weapons alone, but on systems, people, laws, and trust that function long after individual operations end.

Community Engagement in National Security

Community engagement is a cornerstone of modern national security and long-term threat prevention. Contemporary security threats no longer emerge solely from conventional Military confrontation but from complex social, economic, ideological, and criminal networks embedded within civilian populations. Terrorism, transnational crime, cybercrime, violent extremism, illicit trafficking, and internal instability all exploit social environments. As a result, national security can no longer be sustained solely through state institutions operating in isolation. It requires the active participation, trust, and cooperation of the community as a first line of detection, prevention, and resilience (Putnam, 2000; Kaldor, 2012).

Community engagement strengthens national security by expanding the intelligence horizon beyond formal agencies. Citizens observe changes in behavior, movement, economic activity, and community tensions long before these indicators reach formal intelligence channels. When trust exists between communities and security institutions, such observations can be shared early, allowing threats to be disrupted before escalation. This concept aligns directly with intelligence-led policing and whole-of-society security models adopted in advanced security systems worldwide (Ratcliffe, 2016; Gill & Phythian, 2018).

Trust is the critical currency of community-based security. Without legitimacy and public confidence, even the most sophisticated intelligence apparatus will be strategically blind. Historical case studies consistently show that where communities fear or distrust security forces, they withhold information, protect actors within their neighborhoods, and, in extreme cases, collaborate with hostile networks (Tyler, 2006). Conversely, where communities view security agencies as professional, fair, and protective of civilian dignity, cooperation increases and threat detection becomes more accurate and timelier.

In Papua New Guinea, the role of community engagement in national security is uniquely significant due to the country's social structure. PNG is characterized by strong kinship ties, clan-based authority, linguistic diversity, and deep-rooted customary governance systems. These social frameworks exert powerful influence over behavior, loyalty, and conflict resolution (Dinnen, 2001). State authority often intersects with, rather than replaces, customary authority. As a result, community leaders, elders, church networks, women's groups, youth associations, and local councils become critical security partners rather than peripheral actors.

Community engagement in PNG therefore operates at the intersection of formal security institutions and informal social regulation mechanisms. When these systems work cooperatively, they form an integrated early-warning network capable of identifying local disputes, criminal movements, radical influences, and external interference before they escalate into national-level threats. When disconnected, security efforts become reactive, fragmented, and vulnerable to manipulation (Gelu, 2013).

One of the most significant contributions of community engagement to national security is in the prevention of violent conflict. Research consistently shows that community dialogue, mediation, and inclusive participation reduce the likelihood of small grievances escalating into violent confrontation (Lederach, 1997; Dinnen & Allen, 2016). In fragile and hybrid governance environments such as PNG, where land disputes, resource conflicts, and political tensions frequently overlap, community-based conflict prevention is not optional—it is essential to national stability.

Community engagement also plays a central role in countering violent extremism and transnational ideological influence. Global evidence demonstrates that extremist recruitment relies heavily on social alienation, grievance exploitation, and misinformation at the community level (United Nations Development Programme [UNDP], 2017). Families, schools, churches, and peer networks are often

the first environments where early signs of radicalization appear. By empowering these local institutions with awareness, reporting pathways, and protective education programs, the state effectively extends its counter-extremism capability into the social fabric itself.

Economic security is another dimension where community engagement directly supports national security. Illicit economies—such as illegal logging, illegal mining, drug trafficking, wildlife trafficking, and people smuggling—are often embedded within rural and urban communities. Residents frequently possess detailed knowledge of these activities but refrain from reporting due to fear of retaliation or mistrust of authorities. When community protection mechanisms, anonymous reporting systems, and witness safeguards are credible, the state gains access to critical intelligence streams that disrupt criminal financing and organized crime infrastructure (UNODC, 2021; APG, 2020).

Women and youth play a particularly strategic role in community-based national security. Women often have access to domestic, social, and relational spaces that are opaque to traditional security surveillance. Youth networks are similarly crucial in identifying peer-driven risks such as drug distribution, gang formation, online radicalization, and cyber-enabled crime (UN Women, 2015). A national security framework that excludes women and youth as active security stakeholders forfeits a substantial proportion of its early-warning and prevention capacity.

Church institutions in Papua New Guinea also hold unparalleled social influence. Churches operate across nearly all provinces, villages, and urban settlements, often with greater reach than state agencies. Their moral authority, counselling systems, and conflict mediation roles place them in a powerful position to support social stability, de-escalation of violence, and early identification of social breakdown indicators (Gelu & Axline, 2008). Strategic partnerships between security agencies and faith-based organizations therefore represent an underutilized pillar of national resilience.

Community engagement must, however, be institutionalized, not improvised. Sustainable engagement requires formal community liaison frameworks, structured outreach programs, culturally competent officers, feedback mechanisms, and protection protocols for community informants. Without these safeguards, community members risk victimization, retaliation, or social exclusion for their cooperation. This fear undermines long-term intelligence flow and erodes trust irreversibly (Tyler, 2006; Gill & Phythian, 2018).

Digital environments now extend community engagement into cyberspace. Social media platforms, encrypted messaging groups, and online forums have become both threat vectors and security assets. Communities increasingly witness cyber harassment, online recruitment, financial fraud, and information warfare in real time. Where cyber awareness and reporting systems exist, these digital communities serve as frontline sensors in national cyber defense (Kello, 2017). For PNG, where digital literacy varies widely, structured cyber community education is fast becoming a national security necessity.

Ultimately, community engagement transforms national security from a centralized enforcement model into a shared social responsibility. It replaces fear-based compliance with partnership-based protection. It redefines citizens not as passive beneficiaries of security, but as active guardians of national stability. This transformation is especially critical in developing security states, where institutional coverage is limited but social networks are dense and influential.

For Papua New Guinea, long-term national security will not be achieved solely through force modernization, legal reform, or intelligence expansion. It will be achieved when communities across provinces, clans, churches, markets, schools, and settlements see national security as their own responsibility, and when the state earns the trust that makes such ownership possible. Community engagement is therefore not only a tactical tool for threat prevention—it is a strategic foundation for national resilience.

Lessons Learned and Preparing PNG for the Future

The national security journey of Papua New Guinea has been shaped by a complex blend of internal vulnerability, regional strategic competition, institutional fragility, and resilient community foundations. The lessons learned from past security challenges are not merely historical reflections; they are strategic assets that must inform the country's preparation for future threats. In a rapidly evolving global security environment, states that fail to convert past experience into forward-looking policy remain structurally exposed to repeat crises (Kaldor, 2012; Bruneau & Boraz, 2007).

One of the most persistent lessons in Papua New Guinea's security experience is that instability is rarely imported in isolation. External threats consistently exploit internal weaknesses. Transnational crime, economic sabotage, cyber intrusion, foreign intelligence penetration, and illicit resource

exploitation all thrive in governance vacuums, weak law enforcement, poor border control, and fractured political legitimacy (Dinnen, 2001; Firth, 2018). This reinforces a central national security truth: internal resilience is the first and most decisive layer of national defense.

Another enduring lesson is the cost of reactive security policy. Historically, security responses in PNG have often been activated after crises have already escalated, whether during electoral violence, urban crime surges, border incursions, or civil unrest. Reactive security is expensive, destabilizing, and politically corrosive. Preventive security, by contrast, requires earlier investment in intelligence forecasting, community engagement, institutional strengthening, and regional coordination (Ratcliffe, 2016; Gill & Phythian, 2018).

Intelligence failure remains one of the most consequential risks in future preparedness. Global intelligence history demonstrates that most large-scale security breakdowns occur not because information was absent, but because it was misinterpreted, delayed, politicized, or ignored (Heuer, 1999). For PNG, where intelligence systems remain under-resourced and fragmented, the lesson is clear: national survival in the twenty-first century depends not on the quantity of information collected, but on the quality of national sense-making.

Leadership integrity has also emerged as a defining security variable. Weak leadership erodes discipline, enables corruption, weakens command authority, and compromises intelligence protection. Strong leadership, by contrast, stabilizes institutions even when resources are scarce (Westoby & Dowden, 2010). For future preparedness, leadership development within PNG's defense, police, and intelligence sectors must not only prioritize tactical competence but also ethical resilience, political neutrality, and strategic foresight.

Another central lesson concerns the inseparability of economic security and national security. PNG's vulnerability to illegal logging, illegal mining, narcotics trafficking, human trafficking, and financial crime has demonstrated that economic predation weakens state authority just as effectively as armed insurgency (APG, 2020; UNODC, 2021). Preparing for the future therefore requires a national security doctrine that integrates financial intelligence, anti-corruption enforcement, trade monitoring, and resource governance as core security functions rather than peripheral regulatory tasks.

The increasing weaponization of cyberspace presents another defining lesson for future preparedness. Cybercrime, disinformation campaigns, digital espionage, and financial fraud now operate faster than traditional law enforcement response cycles. Kello (2017) argues that cyberspace has become a

permanent battlespace where strategic influence is exercised below the threshold of open conflict. For Papua New Guinea, where digital infrastructure is expanding faster than cyber defense capacity, future readiness depends on accelerated cyber training, digital forensics, secure government networks, and community-level cyber awareness.

Papua New Guinea's social structure also yields important lessons for future national security planning. Clan loyalties, village authority systems, and church networks remain among the most powerful stabilizing forces in the country. Attempts to impose purely centralized Western security models without integrating customary governance have repeatedly produced limited results (Dinnen & Allen, 2016; Gelu, 2013). Future preparedness therefore requires hybrid governance models that legally and operationally align formal institutions with customary authority structures.

The regional security environment provides further instructive lessons. Strategic competition in the Indo-Pacific is intensifying, with small states increasingly exposed to coercive diplomacy, infrastructure leverage, debt pressure, and intelligence maneuvering by major powers (Firth, 2018). For PNG, future preparedness requires a disciplined foreign policy posture anchored in sovereignty protection, diversified partnerships, intelligence independence, and strategic neutrality supported by strong internal institutions.

A further lesson concerns the strategic role of youth in national security. Demographic trends across the Pacific indicate that young populations will dominate political, economic, and security trajectories for decades (UNDP, 2017). Where youth are excluded from economic participation and civic engagement, they become vulnerable to criminal recruitment, political manipulation, and social unrest. Preparing PNG for the future therefore requires the deliberate militarization of discipline without the radicalization of identity: youth leadership programs, digital skills training, national service pathways, and civic education embedded within national resilience strategy.

Women's participation in national security has also emerged as a critical preparedness lesson. Empirical evidence consistently demonstrates that peace processes, community security, intelligence collection, and post-conflict stabilization are more durable where women are actively integrated into security planning and leadership (UN Women, 2015). For PNG, where women already exert strong informal security influence within families, markets, churches, and communities, formal integration into security architecture represents a force multiplier that remains underutilized.

Preparing Papua New Guinea for the future therefore requires a fundamental shift from crisis-driven security management to foresight-driven national resilience. Strategic foresight involves scenario forecasting, stress-testing institutions, wargaming non-traditional threats, and embedding long-term risk analysis into national planning cycles. This approach enables states to anticipate disruptive shocks rather than simply endure them (Kaldor, 2012; Bruneau & Boraz, 2007).

The final lesson is that national security is ultimately a collective enterprise. Institutions, intelligence agencies, political leadership, civil society, churches, businesses, youth, women, and communities are all co-architects of national survival. Preparedness cannot be outsourced to a single agency or uniformed service. It must be cultivated as a national culture—one that values vigilance, integrity, unity, and sacrifice for future generations.

For Papua New Guinea, the path forward is neither abstract nor distant. It is already unfolding through digital transformation, regional pressure, population growth, climate stress, urbanization, and shifting geopolitical alignments. The ultimate measure of preparedness will not be whether PNG avoids every crisis, but whether it acquires the institutional reflexes, intelligence discipline, and societal cohesion to absorb shocks without collapsing into instability.

In this sense, national security becomes not merely the protection of borders and infrastructure, but the preservation of national identity, sovereignty, dignity, and generational continuity. Preparing for the future is not a single policy choice—it is a permanent national posture.

References

ADB. (2020). *Papua New Guinea energy sector assessment.* Asian Development Bank.

Allen, M., & Hasnain, Z. (2019). *Resource projects and governance in PNG.* World Bank Pacific Studies.

Allison, G. (2017). *Destined for war: Can America and China escape Thucydides's trap?* Houghton Mifflin Harcourt.

Asia/Pacific Group on Money Laundering. (2020). *Mutual evaluation report: Papua New Guinea.* APG Secretariat.

Australian Cyber Security Centre. (2022). *Annual cyber threat report.* ACSC.

Australian Strategic Policy Institute. (2020). *The geopolitics of the Pacific Islands.* ASPI Publications.

Australian Strategic Policy Institute. (2021). *Pacific maritime security: Strategic cooperation in the region.* ASPI Publications.

Baker, J. (2019). *Interagency coordination in complex security environments.* Oxford University Press.

Balgos, B., & Figueroa, A. (2021). Crisis preparedness and disaster-response systems in the Pacific region. *Journal of Pacific Security, 6*(2), 44–61.

Bateman, S. (2022). Naval competition in the South Pacific. *Contemporary Southeast Asia, 44*(2), 215–233.

Bateman, S., & Bergin, A. (2019). Indo-Pacific maritime security: Challenges and cooperation. ASPI.

Betts, R. K. (2007). *Enemies of intelligence: Knowledge and power in American national security.* Columbia University Press.

Betts, R. K. (2015). *American strategy: Issues and alternatives.* Routledge.

Boe Declaration on Regional Security. (2018). Pacific Islands Forum.

Borum, R. (2015). Assessing threats of targeted violence: A behavioral approach. *Journal of Threat Assessment and Management, 2*(4), 243–258.

Bruneau, T. C., & Boraz, S. C. (2007). *Reforming intelligence: Obstacles to democratic control and effectiveness.* University of Texas Press.

Bruneau, T. C., & Matei, F. (2013). *The Routledge handbook of civil-Military relations.* Routledge.

CERT-PNG. (2023). *Cybersecurity incidents in Papua New Guinea.* Department of Information and Communications Technology.

Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats.* Penguin.

Connolly, P. (2020). The Belt and Road comes to Papua New Guinea: Chinese economic statecraft and the Pacific. ANU Open Research Repository. JSTOR

Cranford, J. (2022). Scenario-based Military training: Lessons for small-state defence forces. *Security Studies Review, 18*(1), 72–90.

Crichton, M. T., Flin, R., & Rattray, W. A. (2014). *Situational awareness and decision-making in crisis response.* Palgrave Macmillan.

Department of Defence (Papua New Guinea). (2013). *Defence White Paper.* Government of Papua New Guinea.

Department of Defence. (2020). *Insider threat mitigation guidance.* Australian Government.

Department of Foreign Affairs and Trade (DFAT). (n.d.). Australia and Papua New Guinea 1966–1969 (historical overview). Australian Government. DFAT

Dibb, P., & Brabin-Smith, R. (2017). Australia's management of strategic risk in the Indo-Pacific. ASPI.

Dinnen, S. (2001). *Law and order in a weak state: Crime and politics in Papua New Guinea.* University of Hawaii Press.

Dinnen, S., & Allen, M. (2016). *State absence and informal security in the Pacific.* ANU Press.

Dinnen, S., Gelu, A., & Batley, J. (2013). *Politics, security and development in small states: The case of Papua New Guinea.* ANU Press.

Dinnen, S., & Walton, G. (2020). *Precarious order: Crime, policing and security in Papua New Guinea.* ANU Press.

Dobell, G. (2021). *The Pacific step-up and regional security.* Australian Strategic Policy Institute.

Dornan, M. (2021). Infrastructure, digital connectivity and security in the Pacific. *Asia & the Pacific Policy Studies, 8*(2), 232–245.

Dornan, M., & Newton Cain, T. (2022). *Pacific island security and strategic competition.* ANU Press.

Firth, S. (2018). *Australia in international politics: An introduction to Australian foreign policy.* Routledge.

Firth, S., & Yon, D. (2022). Pacific regional security: Emerging trends and challenges. *Pacific Affairs, 95*(1), 31–52.

Fraenkel, J., & Smith, G. (2021). *The geopolitics of the Pacific Islands.* Oxford University Press.

Fry, G., & Tarte, S. (2015). *The New Pacific diplomacy.* ANU Press.

Gelu, A. (2013). *Governance and security in Papua New Guinea.* National Research Institute.

Gelu, A., & Axline, W. A. (2008). *Church and state in Papua New Guinea.* ANU Press.

Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world (2nd ed.).* Polity Press.

Goddard, M. (2020). State authority, local justice, and security in Papua New Guinea. *Oceania, 90*(3), 349–364.

Government of Papua New Guinea. (2013). *National security policy 2013–2030.* Port Moresby: Department of Prime Minister & NEC.

Government of Papua New Guinea. (2021). *National cyber security strategy.* Port Moresby: Department of ICT.

Government of Papua New Guinea. (2023). *Medium Term Development Plan IV 2023–2027.* Port Moresby.

Government of Papua New Guinea, Department of Information and Communications Technology. (2024). *PNG National Cyber Security Strategy 2024–2030.* ICT Papua New Guinea.

Greitzer, F., Kangas, L., Noonan, C., & Dalton, A. (2021). Behavioral indicators of insider threat. *Security Informatics, 10*(1), 1–18.

Heuer, R. J. (1999). *Psychology of intelligence analysis.* Central Intelligence Agency.

Henderson, J., & Reilly, B. (2021). *Great power competition in the Pacific Islands.* Lowy Institute.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars.* Potomac Institute for Policy Studies.

Howes, S., Wira, D., & Swan, A. (2020). PNG economic development and public sector capacity. ANU Press.

Howes, S. (2020). PNG economic infrastructure challenges. ANU Development Policy Centre.

INTERPOL. (2022). *Global cybercrime and financial crime trends in the Pacific.* INTERPOL Strategic Analysis Unit.

Jackson, R., & Sorensen, G. (2016). *Introduction to international relations: Theories and approaches.* Oxford University Press.

Kaldor, M. (2012). *New and old wars: Organised violence in a global era (3rd ed.).* Polity Press.

Kello, L. (2017). *The virtual weapon and international order.* Yale University Press.

King, P. (2016). *West Papua and Indonesia since Suharto.* UNSW Press.

Klare, M. (2012). *The race for what's left: The global scramble for the world's last resources.* Metropolitan Books.

Lederach, J. P. (1997). *Building peace: Sustainable reconciliation in divided societies.* United States Institute of Peace Press.

Lowenthal, M. (2020). *Intelligence: From secrets to policy (8th ed.).* CQ Press.

May, R. J. (2018). *State and society in Papua New Guinea.* ANU Press.

McKenna, M. (2019). Women, peace and community resilience in PNG. *Journal of Pacific Studies, 39*(2), 44–62.

Medcalf, R. (2020). *Indo-Pacific empire: China, America and the contest for the world's pivotal region.* Manchester University Press.

Meloy, J. R., & Hoffman, J. (2021). *International handbook of threat assessment (2nd ed.).* Oxford University Press.

Mearsheimer, J. (2021). *The tragedy of great power politics (Updated ed.).* W. W. Norton.

Mitnick, K., & Simon, W. (2011). *The art of deception.* Wiley.

Nye, J. S. (2010). *Cyber power.* Harvard Kennedy School, Belfer Center.

Nye, J. S. (2018). Cyber power and national security. *Foreign Affairs, 97*(1), 19–28.

PNG ICT Authority. (2020). *National ICT policy.*

PNG National Research Institute. (2019). *Digital governance and security in PNG.*

Powell, J. (2020). Economic statecraft in the Pacific. *Journal of Strategic Studies, 43*(5), 712–736.

Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community.* Simon & Schuster.

Ratcliffe, J. H. (2016). *Intelligence-led policing (2nd ed.).* Routledge.

Regan, A. (2005). Bougainville: The conflict and the peace process. *Development Bulletin (Canberra), 67,* 96–98.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

Rose-Ackerman, S., & Palifka, B. (2016). *Corruption and government: Causes, consequences, and reform (2nd ed.).* Cambridge University Press.

Rosenbach, E., & Peritz, A. (2009). Confrontation or collaboration? Congress and the intelligence community. Harvard Belfer Center.

Sandline and related analysis: Dorney, S. & others. *Challenging the State: the Sandline Affair in Papua New Guinea.* ANU Open Research Repository.

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with AI-enabled malware and intrusion detection. *arXiv preprint.*

Shaw, E., & Sellers, L. (2015). Application of the critical pathway approach to insider threat. *Studies in Intelligence, 59*(2), 1–15.

Shelley, L. (2014). *Dirty entanglements: Corruption, crime, and terrorism.* Cambridge University Press.

Transparency International. (2023). *Corruption perceptions index: Papua New Guinea.* Transparency International.

Tyler, T. R. (2006). *Why people obey the law.* Princeton University Press.

UNCTAD. (2021). *Review of maritime transport 2021.* United Nations Conference on Trade and Development.

United Nations & Government of PNG. (2019). *PNG National Disaster Risk Management Framework 2017–2030.* UNDP.

United Nations Development Programme. (2017). *Preventing violent extremism through inclusive development.* UNDP.

United Nations Office on Drugs and Crime. (2021). *Global study on organized crime.* UNODC.

UN Women. (2015). *Preventing conflict, transforming justice, securing the peace.* United Nations.

Wallis, J. (2019). *Pacific governance and security vulnerabilities.* Australian National University Press.

Wallis, J. (2019). *Pacific security cooperation and strategic alignment.* Australian National University Press.

Wardle, C., & Derakhshan, H. (2017). *Information disorder.* Council of Europe.

Webb-Gannon, C. (2014). *Morning star rising: The politics of decolonisation in West Papua.* University of Hawaii Press.

White, H. (2019). *How to defend Australia.* La Trobe University Press.

Westoby, P., & Dowden, A. (2010). *Leadership and institutional failure in fragile states.* Palgrave Macmillan.

Zorn, J. (2021). Melanesian organizational culture and security. *Pacific Affairs, 94*(4), 550–567.

Zorn, J. (2021). Melanesian policing partnerships and shared security. *Pacific Affairs, 94*(4), 512–530.